

## CONGRUENCES OF MODELS OF ELLIPTIC CURVES

QING LIU AND HUAJUN LU

ABSTRACT. Let  $\mathcal{O}_K$  be a complete discrete valuation ring with field of fractions  $K$ . Let  $E$  be an elliptic curve over  $K$  and let  $L/K$  be a finite Galois extension. Denote by  $\mathcal{X}'$  the minimal regular model of  $E_L$  over  $\mathcal{O}_L$ . We show that the special fibers of the minimal Weierstrass model and the minimal regular model of  $E$  over  $\mathcal{O}_K$  are determined by the infinitesimal fiber  $\mathcal{X}'_m$  together with the action of  $\text{Gal}(L/K)$ , when  $m$  is big enough (depending on the minimal discriminant of  $E$  and the different of  $L/K$ ).

## 1. INTRODUCTION

Let  $\mathcal{O}_K$  be a discrete valuation ring with field of fractions  $K$ . Let  $E$  be an elliptic curve over  $K$ . The minimal (projective) regular model  $\mathcal{X}$  of  $E$  over  $\mathcal{O}_K$  encodes interesting arithmetical invariants of  $E$  (e.g. the conductor of  $E$ , and the smooth locus of  $\mathcal{X}$  is the Néron model of  $E$ ). It is then important to be able to determine this model. Let  $L/K$  be a finite Galois extension with Galois group  $G$ . Let  $\mathcal{X}'$  be the minimal regular model of  $E_L$  over  $\mathcal{O}_L$ . By the uniqueness of minimal regular models,  $G$  acts on the  $\mathcal{O}_K$ -scheme  $\mathcal{X}'$ . It is well known that there exists  $L$  as above such that  $\mathcal{X}'$  is semi-stable. When  $L/K$  is moreover tamely ramified, Viehweg [28] (for curves of any genus  $\geq 1$ ) showed that the special fiber  $\mathcal{X}_0$  of  $\mathcal{X}$  is determined by the action of  $G$  on the special fibers of  $\mathcal{X}'$ .

In the present work, we consider wildly ramified extensions  $L/K$  for elliptic curves. We will *not suppose*  $E_L$  has semi-stable reduction, even though this is probably the most interesting situation. For any  $\mathcal{O}_K$ -scheme  $\mathcal{Z}$  and for any integer  $N \geq 0$ , we will denote as usual

$$\mathcal{Z}_N := \mathcal{Z} \times_{\text{Spec } \mathcal{O}_K} \text{Spec}(\mathcal{O}_K/\pi^{N+1}\mathcal{O}_K)$$

where  $\pi$  is a uniformizing element of  $\mathcal{O}_K$ . For any  $\mathcal{O}_L$ -scheme  $\mathcal{Z}'$ , the infinitesimal fiber  $\mathcal{Z}'_N$  is by definition

$$\mathcal{Z}'_N := \mathcal{Z}' \times_{\text{Spec } \mathcal{O}_K} \text{Spec}(\mathcal{O}_K/\pi^{N+1}\mathcal{O}_K)$$

which is also equal to  $\mathcal{Z}' \times_{\text{Spec } \mathcal{O}_L} \text{Spec}(\mathcal{O}_L/\pi_L^{(N+1)e_{L/K}}\mathcal{O}_L)$ , where  $e_{L/K}$  is the ramification index. In §2, Examples 2.1 and 2.2, we exhibit for any positive integer  $l$ , two elliptic curves over  $K$  having isomorphic  $(\mathcal{X}'_l, G)$  but with non-isomorphic special fibers  $\mathcal{X}_0$ . Hence Viehweg's result can not be extended directly to the wild ramification case. A natural question, attributed to B. Mazur and pointed out to us by W. McCallum, is whether  $\mathcal{X}_0$  is determined

by  $(\mathcal{X}'_\ell, G)$  for  $\ell$  big enough. We give a positive answer in the present work:

**Theorem 7.3** *Let  $N \geq 0$ . Let  $\Delta$  be the minimal discriminant of  $E$ . Let  $\mathfrak{D}_{L/K}$  the different of  $L/K$ . Then the scheme  $\mathcal{X}_N$  is determined by the  $G$ -action on  $\mathcal{X}'_{N+\ell}$  for  $\ell = 2v_K(\Delta) + 12[v_K(\mathfrak{D}_{L/K})] + 18$ .*

If the reduction type of  $E$  is neither  $I_r^*$  nor  $I_r$  ( $r > 0$ ) (e.g.  $E$  has potentially good reduction), we can find such  $\ell$  depending only on  $[v_K(\mathfrak{D}_{L/K})]$ . Note that  $[v_K(\mathfrak{D}_{L/K})]$  is bounded by a constant depending only on the absolute ramification index of  $K$  and on the degree  $[L : K]$  when  $\text{char}(K) = 0$ .

At this stage, let us precise the meaning of “ $\mathcal{X}_N$  is determined by the  $G$ -action on  $\mathcal{X}'_{N+\ell}$ ”. Let  $E_o$  be an elliptic curve over  $K_o$ , let  $L_o$  be finite Galois extensions of  $K_o$  of the same Galois group  $G$ . Let  $\mathcal{X}_o$  be the minimal regular models of  $E_o$  over  $\mathcal{O}_{K_o}$  and let  $\mathcal{X}'_o$  be the respective minimal regular models of  $(E_o)_{L_o}$  over  $\mathcal{O}_{L_o}$ . We say that

$$\mathcal{X}_N \text{ is determined by the } G\text{-action on } \mathcal{X}'_{N+\ell}$$

if the existence of  $G$ -equivariant isomorphisms

$$\mathcal{O}_L/\pi^{N+\ell}\mathcal{O}_L \simeq \mathcal{O}_{L_o}/\pi_o^{N+\ell}\mathcal{O}_{L_o}, \quad \mathcal{X}'_{N+\ell} \simeq \mathcal{X}'_{o,N+\ell}$$

implies that  $\mathcal{X}_N \simeq \mathcal{X}_{o,N}$ . We define similar notion for minimal Weierstrass models.

Let us present the organization of this paper. In §2 we construct examples mentioned above. The second example will also be used to show the necessity of the hypothesis  $\text{char}(K) = 0$  in Theorem 5.9.

Section 3 is a technical preliminary work. We study the invariants of a finitely generated  $\mathcal{O}_L$ -module under a semi-linear action. In §4 and 5, we study the minimal Weierstrass model  $\mathcal{W}$  of  $E$  over  $\mathcal{O}_K$ , as well as the fibers  $\mathcal{W}_N$  in relation with the action of  $G$  on the minimal Weierstrass model of  $E_L$  over  $\mathcal{O}_L$ .

In §6, we study the relation between  $\mathcal{W}_{N+\ell}$  and  $\mathcal{X}_N$ . More precisely, we show explicitly that a small infinitesimal deformation on a scheme produces a small infinitesimal deformation on the blowup (Theorem 6.4).

The main result Theorem 7.3 is proved in §7 using the connection between  $\mathcal{X}$  and the minimal Weierstrass model  $\mathcal{W}$  of  $E$ . The proof can be divided into three steps:

(1) Let  $\mathcal{W}'$  be the minimal Weierstrass model of  $E_L$  over  $\mathcal{O}_L$ . We show that the  $G$ -action on  $\mathcal{X}'_{N+\ell_1}$  determines the  $G$ -action on  $\mathcal{W}'_{N+\ell_1}$  in Proposition 7.2.

(2) We prove that  $\mathcal{W}_{N+\ell_2}$  is determined by the  $G$ -action on  $\mathcal{W}'_{N+\ell_1}$  if  $\ell_2 \ll \ell_1$  (Theorem 5.6). This is the crucial part. We can choose  $\ell_1 - \ell_2$  such that it depends only on the valuation of the discriminant of  $L/K$ . When

$\text{char}(K) = 0$ , the difference  $\ell_1 - \ell_2$  depends only on the absolute ramification index of  $K$ .

(3) Finally, by studying the effect of an infinitesimal deformation on the blowups (Theorem 6.4), we show that  $\mathcal{X}_N$  is determined by  $\mathcal{W}_{N+\ell}$  some  $\ell \geq 0$  (Corollary 6.7).

We also proved a converse of Theorem 7.3: the  $G$ -action on  $\mathcal{X}'_N$  can be determined by  $\mathcal{X}'_{N+\ell'}$  for another positive integer  $\ell'$  (Proposition 7.6).

As we always work with pointed schemes  $\mathcal{W}'_N, \mathcal{X}'_N$ , in the last section, we show that a Galois invariant section of such a fiber lifts to a Galois invariant section over  $S$  when  $N \gg 0$  (Proposition 8.1). If we use Néron models, then we get an explicit bound (Proposition 8.4)

We would like to mention that the present work is similar to (and inspired by) Chai-Yu and Chai's articles [6], [5] where they dealt with Néron models of tori and abelian varieties, though we use a more down-to-earth method. It is shown in [5], Theorem 7.6, that for any abelian variety  $A$  over  $K$ , the infinitesimal fiber  $\mathcal{A}_N$  of the Néron model  $\mathcal{A}$  of  $A$  over  $\mathcal{O}_K$  is determined by the  $G$ -action on  $\mathcal{A}'_{N+\ell}$  (where  $\mathcal{A}'$  is the Néron model of  $A_L$  over  $\mathcal{O}_L$ ) for  $\ell$  big enough and depending on  $\mathcal{A}'$ . Related to his work is the computation, in case of elliptic curves, of the base change conductor (§4.12).

This work grew from the first part of the second named author's Ph.D thesis. He thanks the Institut de Mathématiques de Bordeaux for the nice working environment and financial support.

**Convention** Through this work,  $K$  will denote a discrete valuation field with residue field  $k$  of characteristic  $p \geq 0$ ,  $\mathcal{O}_K$  is the valuation ring of  $K$ ,  $\pi$  or  $\pi_K$  denotes a uniformizing element of  $K$  and  $v_K$  is the normalized valuation ( $v_K(\pi) = 1$ ),  $E$  is an elliptic curve over  $K$  and  $\mathcal{X}$  (resp.  $\mathcal{W}$ ) denotes its minimal projective regular (resp. minimal Weierstrass) model over  $\mathcal{O}_K$ .

The residue field  $k$  will be supposed to be *perfect* starting §5.<sup>1</sup>

We will denote by  $L/K$  a finite Galois extensions with Galois group  $G$ . As usual, the different of  $L/K$  will be denoted by  $\mathfrak{D}_{L/K}$ . The ramification index of  $L/K$  at some maximal ideal  $\mathfrak{p}$  of  $\mathcal{O}_L$  will be denoted by  $e_{L/K}$ . The exponent of  $\mathfrak{D}_{L/K}$  at  $\mathfrak{p}$  will be denoted by  $v_L(\mathfrak{D}_{L/K})$ . As  $L/K$  is Galois, these invariants are independent on the choice of  $\mathfrak{p}$ . Sometimes it is convenient to write

$$v_K(\mathfrak{D}_{L/K}) := \frac{v_L(\mathfrak{D}_{L/K})}{e_{L/K}} \in \mathbb{Q}.$$

---

<sup>1</sup>We thank Ivan Fesenko for encourage us to remove the original hypothesis  $k$  algebraically closed.

## 2. TWO EXAMPLES

In this section, we give two examples. The first one shows that, contrarily to the tamely ramified case, for any  $l \geq 0$ , there exist  $K$  and  $E/K$  such that the special fiber  $\mathcal{X}_0$  (resp.  $\mathcal{W}_1$ ) is not determined by the  $G$ -action on  $\mathcal{X}'_l$  (resp. the infinitesimal fiber  $\mathcal{W}'_1$ ). The second example, of similar nature, shows that in equal characteristic case, there is no bound on  $l$  independent on  $E$  for which Theorem 5.9 holds.

**Example 2.1** Let  $m \geq 1$ . Let  $K = W(\overline{\mathbb{F}}_2)(\pi)$  with  $\pi^{3(2m+1)} = 2$  where  $W(\overline{\mathbb{F}}_2)$  is the Witt ring of  $\overline{\mathbb{F}}_2$ . Let  $E$  be the elliptic curve defined by the equation:

$$y^2 = x^3 + \pi^3.$$

Then  $E$  has good reduction over  $L = K(\sqrt{\pi})$ , with

$$\text{Gal}(L/K) = \langle \sigma \rangle, \quad \sigma(\pi) = -\pi, \quad \mathfrak{D}_{L/K} = 2\sqrt{\pi}\mathcal{O}_L.$$

The smooth model  $\mathcal{X}'$  of  $E_L$  over  $\mathcal{O}_L$  is defined by the equation

$$v^2 + v = u^3,$$

where  $x = \pi\sqrt[3]{4}u$  (note that  $\sqrt[3]{4} \in K$ ) and  $y = \pi^{3/2}(1 + 2v)$ . Hence the action of  $G$  on  $\mathcal{X}'$  is given by:

$$\sigma(u) = u, \quad \sigma(v) = -1 - v.$$

Now let  $E_o$  be the elliptic curve over the same  $K$  defined by the equation:

$$y_o^2 = x_o^3 + (1 + \pi).$$

Then  $E_o$  has good reduction over  $L_o = K(\sqrt{1 + \pi})$ , with

$$\text{Gal}(L_o/K) = \langle \sigma \rangle, \quad \sigma(\sqrt{1 + \pi}) = -\sqrt{1 + \pi}, \quad \mathfrak{D}_{L_o/K} = 2\mathcal{O}_{L_o}.$$

The smooth model  $\mathcal{X}'_o$  of  $E_o$  over  $L_o$  is defined by the equation:

$$v_o^2 + v_o = u_o^3,$$

where  $x_o = (4(1 + \pi))^{1/3}u_o$  with  $(1 + \pi)^{1/3} \in K$  and  $y_o = \sqrt{1 + \pi}(1 + 2v_o)$ . The action of  $G$  on  $\mathcal{X}'_o$  is then given by  $\sigma(u_o) = u_o, \sigma(v_o) = -1 - v_o$ .

Let  $d = 3(2m + 1) - 1$ . It is easy to see that we have an isomorphism

$$\mathcal{O}_L/(2) = \mathcal{O}_L/(\pi^{d+1}) \simeq \mathcal{O}_{L_o}/(\pi^{d+1})$$

which sends  $\sqrt{\pi}$  to  $\sqrt{1 + \pi} - 1$  and which is compatible with the  $G$ -action. Note that  $v_K(\mathfrak{D}_{L/K}) = d + 3/2 \neq v_K(\mathfrak{D}_{L_o/K}) = d + 1$ , hence by Lemma 5.1,  $\mathcal{O}_L/(\pi^{d+2}) \not\simeq \mathcal{O}_{L_o}/(\pi^{d+2})$ . We also have an isomorphism

$$\mathcal{X}'_d \simeq \mathcal{X}'_{o,d}$$

which sends  $u_o$  (resp.  $v_o$ ) to  $u$  (resp.  $v$ ) and which is compatible with the  $G$ -action. However, the special fibers of the regular proper models of  $E$  and  $E_o$  over  $\mathcal{O}_K$  have different Kodaira types: the first curve has type  $I_0^*$  by

Tate's Algorithm, and the second one has type II. Note this example doesn't contradict the conclusion of Theorem 7.3.

Let  $\mathcal{W}$  (resp.  $\mathcal{W}_o$ ) be the minimal Weierstrass model of  $E$  (resp.  $E_o$ ) over  $\mathcal{O}_K$ . Then  $\{1, x, y\}$  and  $\{1, x_o, y_o\}$  are respective Weierstrass basis of  $\mathcal{W}, \mathcal{W}_o$ , and  $\mathcal{X}', \mathcal{X}'_o$  are the respective minimal Weierstrass models over  $\mathcal{O}_L, \mathcal{O}_{L_o}$ . Clearly the special fibers of  $\mathcal{W}, \mathcal{W}_o$  are isomorphic, but using Lemma 5.4, we can show that  $\mathcal{W}_1 \not\cong \mathcal{W}_{o,1}$ .

**Example 2.2** Fix  $m \geq 1$  and let  $r = 1, 3$ . Let  $k$  be an algebraically closed field of characteristic 2 and  $K = k((t))$ . Consider the elliptic curve  ${}_rE$  :

$$y^2 + t^{3m}y = x^3 + t^r,$$

whose  $j$ -invariant is 0 and whose discriminant has valuation equal to  $12m$ . The above equation defines a minimal Weierstrass model  ${}_r\mathcal{W}$  of  ${}_rE$  over  $k[[t]]$ . Let  $\alpha_r$  be a root of the polynomial  $X^2 + t^{3m}X + t^r$  in  $\overline{K}$  and let  $L_r = K[\alpha_r]$ . Then  ${}_rE_{L_r}$  has a smooth model  ${}_r\mathcal{X}'$  over  $\mathcal{O}_{L_r}$  defined by the equation:

$$y'^2 + y' = x'^3,$$

where  $x = t^{2m}x'$  and  $y = t^{3m}y' + \alpha_r$ . Hence

$$\text{Gal}(L_r/K) = \langle \sigma \rangle, \quad \sigma(\alpha_r) = t^{3m} + \alpha_r; \quad \sigma(x') = x', \quad \sigma(y') = y' + 1.$$

For  $r = 1$ , the model  ${}_1\mathcal{W}$  is regular, hence  ${}_1E$  has reduction type II. The ring of integers  $\mathcal{O}_{L_1}$  is  $k[[t, \alpha_1]] \cong k[[t]][X]/(X^2 - t^{3m}X + t)$ . For  $r = 3$ , the curve  ${}_3E$  has reduction type  $I_0^*$  by Tate's Algorithm. The ring of integers  $\mathcal{O}_{L_3}$  is  $k[[t, \alpha_3/t]] \cong k[[t]][X]/(X^2 - t^{3m-1}X + t)$ .

We have  $G$ -equivariant isomorphisms

$$\mathcal{O}_{L_1}/(t^{3m-1}) \cong \mathcal{O}_{L_3}/(t^{3m-1})$$

which sends  $\overline{\alpha}_1$  to  $\overline{\alpha}_3/t$ , and

$$({}_1\mathcal{X}')_d \cong ({}_3\mathcal{X}')_d, \quad d = 3m - 2.$$

Hence the  $l$  in Theorem 5.9 must be bigger than  $3m - 1$  and it tends to infinity if  $m$  does.

### 3. SEMI-LINEAR $\mathcal{O}_L[G]$ -MODULES

Let  $L/K$  be a finite Galois extension with Galois group  $G$ . Denote the integral closure of  $\mathcal{O}_K$  in  $L$  by  $\mathcal{O}_L$ . The aim of this section is, given a semi-linear  $\mathcal{O}_L[G]$ -module  $M$ , to compare  $M^G/\pi^{N+1}M^G$  with the image of  $(M/\pi^{N+1+r}M)^G$  in  $(M/\pi^{N+1}M)^G$  (Proposition 3.9). The result is used in §4 and §5.

**Definition 3.1** A *semi-linear  $\mathcal{O}_L[G]$ -module* is an  $\mathcal{O}_L$ -module  $M$  endowed with an action of  $G$  such that

- (1)  $g(x_1 + x_2) = g(x_1) + g(x_2)$  for all  $x_1, x_2 \in M$ ,
- (2)  $g(ax) = g(a)g(x)$  for all  $a \in \mathcal{O}_L, x \in M$  and  $g \in G$ .

A *morphism*  $\phi$  between two semi-linear  $\mathcal{O}_L[G]$ -modules  $M$  and  $N$  is an  $\mathcal{O}_L$ -morphism which is  $G$ -equivariant (i.e.  $\phi(gx) = g\phi(x), \forall g \in G, \forall x \in M$ ).

Let us recall the following well known lemma (see for instance [22], Proposition 1(a)):

**Lemma 3.2. (Speiser's lemma)** *Let  $V$  be a semi-linear  $L[G]$ -vector space. Then the canonical morphism of semi-linear  $L[G]$ -vector spaces*

$$L \otimes_K V^G \rightarrow V$$

*is an isomorphism.*

**Proposition 3.3.** *Let  $M$  be a semi-linear  $\mathcal{O}_L[G]$ -module. Let*

$$\varphi : \mathcal{O}_L \otimes_{\mathcal{O}_K} M^G \rightarrow M$$

*be the natural morphism of semi-linear  $\mathcal{O}_L[G]$ -modules.*

- (1) *If  $M$  is flat over  $\mathcal{O}_L$ , then  $\varphi$  is injective and  $\text{rank}_{\mathcal{O}_K} M^G = \text{rank}_{\mathcal{O}_L} M$ .*
- (2) *The cokernel of  $\varphi$  is killed by the different ideal  $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$  of  $\mathcal{O}_L$  over  $\mathcal{O}_K$ .*

*Proof.* (1) comes from 3.2 by tensoring  $\varphi$  by  $L$ .

(2) We will first prove the property for monogeneous extensions  $\mathcal{O}_L/\mathcal{O}_K$ . We will deal with the general case first by reducing to the case when  $\mathcal{O}_K$  is complete, and then achieve the proof by induction on the order  $|G|$  of  $G$ .

**Step 1.** Consider  $\mathcal{O}_L[G]$  as a semi-linear  $G$ -module defined by

$$\sigma * \left( \sum_{\tau \in G} \lambda_\tau \cdot \tau \right) = \sum_{\tau \in G} \sigma(\lambda_\tau) \cdot (\sigma\tau).$$

Then  $M$  is a quotient of a direct sum of copies of  $\mathcal{O}_L[G]$ . Therefore it is enough to prove the proposition when  $M = \mathcal{O}_L[G]$ . Denote by

$$t = \sum_{\sigma \in G} \sigma \in \mathcal{O}_L[G].$$

For any  $b \in \mathcal{O}_L$ , we have  $t * b = \sum_{\sigma} \sigma(b) \cdot \sigma \in M^G$ .

Suppose  $\mathcal{O}_L = \mathcal{O}_K[\theta]$  for some  $\theta \in \mathcal{O}_L$ . Let  $P(X) \in \mathcal{O}_K[X]$  be the monic minimal polynomial of  $\theta$ . Then  $\mathcal{O}_L \simeq \mathcal{O}_K[X]/(P(X))$ . We have a decomposition in  $\mathcal{O}_L[X]$ :  $P(X) = (X - \theta)f(X)$  and

$$f(X) = b_{n-1}X^{n-1} + b_{n-2}X^{n-2} + \cdots + b_0 \in \mathcal{O}_L[X].$$

Let  $g := \sum_{0 \leq i \leq n-1} b_i \cdot (t * \theta^i) \in \mathcal{O}_L \otimes M^G$  and let  $e$  be the unit element of  $G$ . Then

$$g = \sum_{\sigma \in G} \sum_i b_i \sigma(\theta)^i e = \sum_{\sigma \in G} f(\sigma(\theta)) e = f(\theta) \cdot e = P'(\theta) \cdot e.$$

For any  $\sigma \in G$ ,

$$P'(\theta)\sigma = (P'(\theta)\sigma(P'(\theta))^{-1}) \cdot \sigma * (P'(\theta) \cdot e) \in \mathcal{O}_L \otimes_{\mathcal{O}_K} M^G.$$

So  $P'(\theta)M \subseteq \mathcal{O}_L \otimes_{\mathcal{O}_K} M^G$  and the proposition is proved in this case as the different of  $\mathcal{O}_L/\mathcal{O}_K$  is generated by  $P'(\theta)$ .

**Step 2.** We reduce to the case when  $\mathcal{O}_K$  is complete. Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  be the maximal ideals of  $\mathcal{O}_L$ . Let  $D_i$  be the decomposition group at  $\mathfrak{p}_i$  and let  $\widehat{\mathcal{O}}_L := \mathcal{O}_L \otimes_{\mathcal{O}_K} \widehat{\mathcal{O}}_K$ . Then

$$\widehat{\mathcal{O}}_L = \bigoplus_{1 \leq i \leq n} \widehat{\mathcal{O}}_{L, \mathfrak{p}_i}$$

and  $\widehat{\mathcal{O}}_{L, \mathfrak{p}_i}$  is Galois of group  $D_i$  over  $\widehat{\mathcal{O}}_K$ . Denote by  $\widehat{M} = \widehat{\mathcal{O}}_L \otimes_{\mathcal{O}_L} M$ . Let  $M_i = \widehat{\mathcal{O}}_{L, \mathfrak{p}_i} \otimes_{\mathcal{O}_L} M$ . Then  $\widehat{M} = \bigoplus_i M_i$  and the projection map  $\widehat{M} \rightarrow M_i$  induces an isomorphism  $\widehat{M}^G \simeq M_i^{D_i}$ . The map  $\widehat{\mathcal{O}}_L \otimes_{\widehat{\mathcal{O}}_K} \widehat{M}^G \rightarrow \widehat{M}$  can be identified with the direct sum of the maps

$$\widehat{\mathcal{O}}_{L, \mathfrak{p}_i} \otimes_{\widehat{\mathcal{O}}_K} M_i^{D_i} \rightarrow M_i.$$

Let  $\theta_1$  be a generator of the different of  $\widehat{\mathcal{O}}_{L, \mathfrak{p}_1} / \widehat{\mathcal{O}}_K$ . Then it extends to a generator  $\theta$  of the different of  $\widehat{\mathcal{O}}_L / \widehat{\mathcal{O}}_K$  by Chinese Remainder Theorem. Suppose we have

$$\theta_1 M_1 \subseteq \widehat{\mathcal{O}}_{L, \mathfrak{p}_1} \otimes_{\widehat{\mathcal{O}}_K} M_1^{D_1}.$$

Then

$$\theta M_1 = \theta_1 M_1 \subseteq \widehat{\mathcal{O}}_{L, \mathfrak{p}_1} \otimes_{\widehat{\mathcal{O}}_K} M_1^{D_1} \simeq \widehat{\mathcal{O}}_{L, \mathfrak{p}_1} \otimes_{\widehat{\mathcal{O}}_K} \widehat{M}^G \subseteq \widehat{\mathcal{O}}_L \otimes_{\widehat{\mathcal{O}}_K} \widehat{M}^G$$

where the middle isomorphism is the inverse of  $\widehat{M}^G \rightarrow M_1^{D_1}$ . This holds similarly for any  $M_i$ , hence  $\theta \widehat{M} \subseteq \widehat{\mathcal{O}}_L \otimes_{\widehat{\mathcal{O}}_K} \widehat{M}^G$ . As

$$\mathfrak{D}_{\widehat{\mathcal{O}}_L / \widehat{\mathcal{O}}_K} = \mathfrak{D}_{\mathcal{O}_L / \mathcal{O}_K} \widehat{\mathcal{O}}_L \quad \text{and} \quad \widehat{\mathcal{O}}_L \otimes_{\mathcal{O}_L} (\mathcal{O}_L \otimes_{\mathcal{O}_K} M^G) = \widehat{\mathcal{O}}_L \otimes_{\widehat{\mathcal{O}}_K} \widehat{M}^G,$$

the proposition will be proved for  $L/K$  if it is proved for  $\widehat{\mathcal{O}}_{L, \mathfrak{p}_1} / \widehat{\mathcal{O}}_K$ .

**Step 3.** Induction on  $|G|$ . Suppose that  $H \subseteq G$  is a normal subgroup and the proposition holds for  $L/L^H$  and  $L^H/K$ . Let  $E = L^H$ . Then

$$\mathfrak{D}_{\mathcal{O}_L / \mathcal{O}_E} M \subseteq \mathcal{O}_L M^E, \quad \mathfrak{D}_{\mathcal{O}_E / \mathcal{O}_K} M^E \subseteq \mathcal{O}_E (M^H)^{G/H} = \mathcal{O}_E M^G.$$

As  $\mathfrak{D}_{\mathcal{O}_L / \mathcal{O}_K} = \mathfrak{D}_{\mathcal{O}_L / \mathcal{O}_E} \cdot (\mathfrak{D}_{\mathcal{O}_E / \mathcal{O}_K} \mathcal{O}_L)$ , the proposition also holds for  $L/K$ .

Now we suppose  $\mathcal{O}_K$  is complete. Then  $\mathcal{O}_L / \mathcal{O}_K$  can be decomposed into successive Galois monogeneous (cyclic) extensions. (See for instance the explanations in [9], proof of Theorem 4.1.) This achieves the proof by Step 1.  $\square$

**Remark 3.4** Proposition 3.3 is sharp for monogeneous Galois extensions  $\mathcal{O}_L = \mathcal{O}_K[\theta]$ . Indeed, let  $M = \mathcal{O}_L[G]$ . Let us show that  $bM \subseteq \mathcal{O}_L \otimes M^G$  implies  $b \in \mathfrak{D}_{L/K}$ . The vectors  $t * \theta^i \in M$ ,  $0 \leq i \leq n-1$ , where  $n$  is the degree of the minimal polynomial  $P(T)$  of  $\theta$ , generate  $\mathcal{O}_L \otimes M^G$ . So

$$b.e = \lambda_0 t * e + \lambda_1 t * \theta + \dots + \lambda_{n-1} t * (\theta^{n-1}), \quad \lambda_i \in \mathcal{O}_L.$$

By expanding  $t * \theta^i$ , we see that for all  $\sigma \neq e$ ,

$$\lambda_0 + \lambda_1 \sigma(\theta) + \dots + \lambda_{n-1} \sigma(\theta)^{n-1} = 0.$$

So the polynomial  $F(T) = \lambda_0 + \lambda_1 T + \cdots + \lambda_{n-1} T^{n-1} \in \mathcal{O}_L[T]$  is divisible by  $f(T) := P(T)/(T - \theta)$ , and

$$b = \lambda_0 + \lambda_1 \theta + \cdots + \lambda_{n-1} \theta^{n-1} = F(\theta) \in f(\theta) \mathcal{O}_L = \mathfrak{D}_{L/K}.$$

When  $\mathcal{O}_L$  is local and the residue extension of  $\mathcal{O}_L/\mathcal{O}_K$  is separable, it is known that  $\mathcal{O}_L$  is monogeneous over  $\mathcal{O}_K$  ([23], III.6, Proposition 12). The next lemma gives a general situation where  $\mathcal{O}_L/\mathcal{O}_K$  is monogeneous.

**Lemma 3.5.** *Suppose that the residue field  $k$  of  $\mathcal{O}_K$  is infinite. Let  $F$  be a finite étale  $K$ -algebra and let  $B$  be the integral closure of  $\mathcal{O}_K$  in  $F$ . Suppose that the residue extensions of  $B/\mathcal{O}_K$  are separable. Then  $B$  is monogeneous over  $\mathcal{O}_K$ .*

*Proof.* (See also [12], Proposition 4.1) Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  be the maximal ideals of  $B$ . Applying [23], *loc. cit.* to the completion  $\widehat{B}_{\mathfrak{p}_i}$ , we see that  $B_{\mathfrak{p}_i}/(\pi) = \widehat{B}_{\mathfrak{p}_i}/(\pi)$  is monogeneous over  $k$ . So  $\text{Spec}(B_{\mathfrak{p}_i}/(\pi))$  admits a closed immersion into  $\mathbb{A}_k^1$ . As  $k$  is infinite, there exists a closed immersion

$$\text{Spec}(B/\pi B) = \coprod_i \text{Spec}(B_{\mathfrak{p}_i}/(\pi)) \hookrightarrow \mathbb{A}_k^1.$$

Let  $\theta \in B$  be a lifting of some generator of  $B/\pi B$  over  $k$ . Then  $B = \mathcal{O}_K[\theta] + \pi B$ . Hence  $B = \mathcal{O}_K[\theta]$  by Nakayama's lemma.  $\square$

**Definition 3.6** Let  $H$  be an  $\mathcal{O}_K$ -module. We define the *exponent*  $\varepsilon(H)$  of  $H$  to be, when it exists, the smallest non-negative integer  $e$  such that  $\pi^e H = 0$ . Note that for any  $\mathcal{O}_L$ -module  $M$ ,  $\varepsilon(M)$  is defined to be its exponent as  $\mathcal{O}_K$ -module.

**Proposition 3.7.** *Let  $M$  be a semi-linear  $\mathcal{O}_L[G]$ -module, flat over  $\mathcal{O}_L$ .*

- (1) *Suppose  $\text{char}(K) = 0$ . Let  $I$  be the inertia of  $G$  at some maximal ideal of  $\mathcal{O}_L$ . Then  $\varepsilon(H^1(G, M)) \leq v_K(|I|)$ .*
- (2) *In general, we have*

$$\varepsilon(H^1(G, M)) \leq 2[v_K(\mathfrak{D}_{L/K})].$$

*Proof.* (1) Let  $\widehat{\mathcal{O}}_K$  be the completion of  $\mathcal{O}_K$ . By the flatness of  $\mathcal{O}_K \rightarrow \widehat{\mathcal{O}}_K$ , we have

$$\varepsilon(H^1(G, M)) = \varepsilon(H^1(G, M) \otimes_{\mathcal{O}_K} \widehat{\mathcal{O}}_K) = \varepsilon(H^1(G, \widehat{\mathcal{O}}_K \otimes_{\mathcal{O}_K} M)).$$

Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  be the maximal ideals of  $\mathcal{O}_L$ . Let  $D$  be the decomposition group of  $\mathfrak{p} := \mathfrak{p}_1$ . Then

$$\widehat{M} := \widehat{\mathcal{O}}_K \otimes_{\mathcal{O}_K} M = \bigoplus_{1 \leq i \leq r} (\widehat{\mathcal{O}}_{L, \mathfrak{p}_i} \otimes_{\mathcal{O}_L} M) \simeq \text{Ind}_D^G(M_1),$$

where  $M_i = \widehat{\mathcal{O}}_{L, \mathfrak{p}_i} \otimes_{\mathcal{O}_L} M$ . By Shapiro's lemma  $H^1(G, \widehat{M}) \simeq H^1(D, M_1)$ . Let  $I$  be the inertia group at  $\mathfrak{p}$ , let  $\mathcal{O}_F = (\widehat{\mathcal{O}}_{L, \mathfrak{p}})^I$ . Then  $\mathcal{O}_F/\widehat{\mathcal{O}}_K$  is étale of Galois group  $D/I$ . The inflation-restriction exact sequence

$$0 = H^1(D/I, M_1^I) \rightarrow H^1(D, M_1) \rightarrow H^1(I, M_1)$$



implies that  $\varepsilon(H^1(G, M)) \leq \varepsilon(H^1(I, M_1))$ . As  $I$  is finite,  $|I|$  kills  $H^1(I, M_1)$  ([23], VIII.1, Corollary 1). This implies the desired inequality.

Note that during this reduction step, we didn't change the valuations of the differentials:  $v_F(\mathfrak{D}_{F/\hat{K}}) = v_L(\mathfrak{D}_{L/K})$ .

(2) As we saw above, we can suppose that  $\mathcal{O}_K$  is complete and  $G$  equal to its inertia group. Consider the  $G$ -equivariant exact sequence of  $\mathcal{O}_L$ -modules:

$$0 \rightarrow \mathcal{O}_L \otimes_{\mathcal{O}_K} M^G \rightarrow M \rightarrow M/(\mathcal{O}_L \otimes_{\mathcal{O}_K} M^G) \rightarrow 0.$$

(The exactness at the left comes from Proposition 3.3(1)). Taking group cohomology, we get the exact sequence

$$H^1(G, \mathcal{O}_L \otimes_{\mathcal{O}_K} M^G) \rightarrow H^1(G, M) \rightarrow H^1(G, M/(\mathcal{O}_L \otimes_{\mathcal{O}_K} M^G)).$$

Let  $\mathfrak{D} = \mathfrak{D}_{L/K}$  and  $e = e_{L/K}$ . By Proposition 3.3, we have

$$\mathfrak{D} \cdot (M/(\mathcal{O}_L \otimes_{\mathcal{O}_K} M^G)) = 0.$$

Hence  $\mathfrak{D} \cdot H^1(G, M/(\mathcal{O}_L \otimes_{\mathcal{O}_K} M^G)) = 0$ . It remains to find the annihilator of  $H^1(G, \mathcal{O}_L \otimes_{\mathcal{O}_K} M^G)$ .

If  $F$  is a free  $\mathcal{O}_K$ -module (with trivial  $G$ -action), then the canonical map  $H^i(G, \mathcal{O}_L) \otimes_{\mathcal{O}_K} F \rightarrow H^i(G, \mathcal{O}_L \otimes_{\mathcal{O}_K} F)$  is an isomorphism for all  $i \geq 0$ . As  $M^G$  is flat over  $\mathcal{O}_K$ , it is an increasing union of free  $\mathcal{O}_K$ -modules. This implies easily that  $H^1(G, \mathcal{O}_L \otimes_{\mathcal{O}_K} M^G) \simeq H^1(G, \mathcal{O}_L) \otimes_{\mathcal{O}_K} M^G$ , hence

$$\text{Ann}(H^1(G, \mathcal{O}_L \otimes_{\mathcal{O}_K} M^G)) = \text{Ann}(H^1(G, \mathcal{O}_L) \otimes_{\mathcal{O}_K} M^G) = \text{Ann}(H^1(G, \mathcal{O}_L)).$$

Let us show that

$$(1) \quad \pi_L^{[v_L(\mathfrak{D})/p]} H^1(G, \mathcal{O}_L) = 0$$

where  $p$  is the residue characteristic of  $K$  (the case  $p = 0$  is considered in Part (1)). Let  $H$  be a normal subgroup of  $G$ . Again using the inflation-restriction exact sequence

$$0 \rightarrow H^1(G/H, \mathcal{O}_{L^H}) \rightarrow H^1(G, \mathcal{O}_L) \rightarrow H^1(H, \mathcal{O}_L)$$

it is easy to show that Equality (1) holds if it holds for  $L^H/K$  and for  $L/L^H$ . Therefore, similarly to the final step of the proof of Proposition 3.3, we are reduced to the case when  $G$  is cyclic. Using Herbrand's quotient as in [21], Remark, pp. 38-39 or [16], p. 508, lines 4-9, we have

$$\text{length}_{\mathcal{O}_K} H^1(G, \mathcal{O}_L) = \text{length}_{\mathcal{O}_K} \mathcal{O}_K / \text{Tr}(\mathcal{O}_L) = [v_K(\mathfrak{D})]$$

Let  $f$  be the degree of the residue extension of  $L/K$ . Then

$$\text{length}_{\mathcal{O}_L} H^1(G, \mathcal{O}_L) \leq [[v_L(\mathfrak{D})/e]/f] = [v_L(\mathfrak{D})/ef].$$

As we can restrict ourselves to non-trivial wild ramified extensions, we have  $ef = [L : K] \geq p$ . Hence  $\pi_L^{[v_L(\mathfrak{D})/p]}$  kills  $H^1(G, \mathcal{O}_L)$ . This implies that  $\pi_L^{v_L(\mathfrak{D})+[v_L(\mathfrak{D})/p]} H^1(G, M) = 0$  and the exponent of  $H^1(G, M)$  is bounded by the smallest integer bigger or equal to  $(v_L(\mathfrak{D}) + [v_L(\mathfrak{D})/2])/e$ . The only case this might fail to be true is when  $v_L(\mathfrak{D}) = e + r$  with  $0 \leq r \leq e - 1$ . As  $L/K$  is wild ramified, this implies that  $L/K$  has no non-trivial intermediate

extensions, hence  $G$  is cyclic (of prime order) and  $[v_L(\mathfrak{D})/p] = 1$ . But then  $(v_L(\mathfrak{D}) + [v_L(\mathfrak{D})/p])/e \leq 2 = 2[v_K(\mathfrak{D})]$ .  $\square$

Note that when  $L/K$  is tamely ramified,  $[v_K(\mathfrak{D})] = [(e-1)/e] = 0$ .

**Remark 3.8** When  $\text{char}(K) = 0$ , one has ([21], Theorem 3)

$$\varepsilon(H^1(G, \mathcal{O}_L)) \leq v_K(p)/(p-1).$$

For any  $\mathcal{O}_K$ -module  $F$  and any  $N \geq 0$ , we will denote

$$F_N = F/\pi^{N+1}F.$$

Let  $M$  be a semi-linear  $\mathcal{O}_L[G]$ -module free over  $\mathcal{O}_L$ . Let  $N \geq 0$ . We would like to compare  $(M_N)^G$  with  $(M^G)_N$ . For all  $m \geq N$ , we have canonical morphisms of  $\mathcal{O}_K$ -modules

$$\begin{array}{ccc} (M^G)_m & \hookrightarrow & (M_m)^G \\ \downarrow & & \downarrow f_{m,N} \\ (M^G)_N & \xrightarrow{f_N} & (M_N)^G \end{array}$$

**Proposition 3.9.** *Let  $M$  be a semi-linear  $\mathcal{O}_L[G]$ -module, flat over  $\mathcal{O}_L$ . Let  $h = 2[v_K(\mathfrak{D}_{L/K})] \geq 0$ . Then for all  $N \geq 1$  and for any  $m \geq N + h$ ,  $(M^G)_N$  is determined by the  $G$ -module  $M_m$ . More precisely, the canonical morphism of  $\mathcal{O}_K$ -modules*

$$(M^G)_N \rightarrow (M_m)^G/(\pi^{N+1})$$

*is an isomorphism.*

*Proof.* The above diagram implies that  $\text{Im} f_N \subseteq \text{Im} f_{m,N}$ . Therefore  $f_N$  induces canonically an injective morphism of  $\mathcal{O}_K$ -modules

$$(M^G)_N \hookrightarrow \text{Im} f_{m,N} \simeq (M_m)^G/(\pi^{N+1}).$$

It remains to show that  $\text{Im} f_{m,N} \subseteq \text{Im} f_N$ . Let us consider the following commutative diagram with horizontal exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \xrightarrow{\cdot\pi^{m+1}} & M & \longrightarrow & M_m \longrightarrow 0 \\ & & \downarrow \cdot\pi^{m-N} & & \downarrow \text{id} & & \downarrow \\ 0 & \longrightarrow & M & \xrightarrow{\cdot\pi^{N+1}} & M & \longrightarrow & M_N \longrightarrow 0 \end{array}$$

where  $\cdot$  means the multiplication and the maps in the rows are the canonical surjection. Then we have the following diagram of long exact sequences by taking group cohomology:

$$\begin{array}{ccccccc} (M^G)_m & \xrightarrow{f_m} & (M_m)^G & \xrightarrow{\Delta_m} & H^1(G, M) & \xrightarrow{\cdot\pi^{m+1}} & H^1(G, M) \\ \text{id} \downarrow & & \downarrow f_{m,N} & & \downarrow \cdot\pi^{m-N} & & \downarrow \text{id} \\ (M^G)_N & \xrightarrow{f_N} & (M_N)^G & \xrightarrow{\Delta_N} & H^1(G, M) & \xrightarrow{\cdot\pi^{N+1}} & H^1(G, M) \end{array}$$

We see that  $\text{Im}f_{m,N} \subseteq \text{Im}f_N$  if and only if  $\Delta_N f_{m,N} = \pi^{m-N} \Delta_m = 0$ . This happens when  $m - N \geq \varepsilon(H^1(G, M))$ . The latter inequality is true by Proposition 3.7.  $\square$

**Remark 3.10** Suppose  $\text{char}(K) = 0$  and  $p > 0$ . Then the ramification filtration of  $G$  has length at most  $v_L(p)/(p-1)$  ([23], IV.2, Exercise 3c). Hence  $v_L(\mathfrak{D}_{L/K}) \leq |G|v_L(p)/(p-1)$  by [23], IV.1, Proposition 4, and we get

$$v_K(\mathfrak{D}_{L/K}) \leq |G|v_K(p)/(p-1).$$

**Remark 3.11** If  $L/K$  is tamely ramified, then  $h = 0$  and we get the well-known equality  $(M_N)^G = (M^G)_N$ .

**Corollary 3.12.** *Under the hypothesis of Proposition 3.9, the canonical homomorphism*

$$\varprojlim_n (M^G)_n \rightarrow \varprojlim_n (M_n)^G = (\varprojlim_n M_n)^G$$

*is an isomorphism.*

#### 4. MINIMAL WEIERSTRASS MODELS

We compare in this section the minimal Weierstrass model of  $E$  over  $\mathcal{O}_K$  with that of  $E_L$  over  $\mathcal{O}_L$ .

**Definition 4.1** Let  $E$  be an elliptic curve over  $K$ . A *Weierstrass model*  $\mathcal{W}$  of  $E$  over  $\mathcal{O}_K$  is a proper flat scheme over  $\text{Spec}\mathcal{O}_K$  with geometrically integral fibers such that the generic fiber  $\mathcal{W}_\eta$  is isomorphic to  $E$  and that the closure  $\epsilon$  in  $\mathcal{W}$  of the origin of  $E$  is contained in the smooth locus of  $\mathcal{W}$ .

Let us recall the correspondence between Weierstrass models and Weierstrass equations ([7], §1 or [15], §9.4.4). Let  $\mathcal{W}$  be a Weierstrass model of  $E$  over  $\mathcal{O}_K$ . Consider the invertible sheaf  $\mathcal{O}_{\mathcal{W}}(n\epsilon)$  in  $\mathcal{W}$ . Then  $\mathcal{O}_{\mathcal{W}}(3\epsilon)$  is very ample, and we can reconstruct the equation of  $\mathcal{W}$  as following. Let  $L(n\epsilon) = \Gamma(\mathcal{W}, \mathcal{O}_{\mathcal{W}}(n\epsilon))$ . For all  $n \geq 1$ ,  $L(n\epsilon)$  is free of rank  $n$  and  $L((n+1)\epsilon)/L(n\epsilon)$  is free of rank 1. So there are basis  $\{1, x\}$  of  $L(2\epsilon)$  and  $\{1, x, y\}$  of  $L(3\epsilon)$ . The images of  $x^3$  and  $y^2$  in  $L(6\epsilon)/L(5\epsilon)$  are both basis. Then we have  $y^2 - \alpha x^3 \in L(5\epsilon)$  for some unit  $\alpha \in \mathcal{O}_K^*$ . Change  $y$  by  $\alpha^{-1}y$  and  $x$  by  $\alpha^{-1}x$ , and we can assume  $\alpha = 1$ . Then the morphism of  $\mathcal{W}$  to  $\mathbb{P}_{\mathcal{O}_K}^2$  associated to the invertible sheaf  $\mathcal{O}_{\mathcal{W}}(3\epsilon)$  with coordinates  $x$  and  $y$  gives an affine Weierstrass equation

$$(2) \quad y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6.$$

We will call such a triplet  $\{1, x, y\}$  a *Weierstrass basis* of  $\mathcal{W}$ . The model  $\mathcal{W}$  is isomorphic to the closed subscheme of  $\mathbb{P}_{\mathcal{O}_K}^2$  defined by the above equation. Denote by  $\Delta(\mathcal{W})$  the discriminant of the above equation. Its valuation depends only on  $\mathcal{W}$  and not on the equation.

**Definition 4.2** If the valuation of the discriminant  $\Delta(\mathcal{W})$  of  $\mathcal{W}$  is minimal among all Weierstrass models of  $E$ , then  $\mathcal{W}$  will be called the *minimal Weierstrass model* of  $E$ . The minimal Weierstrass model of  $E$  over  $\mathcal{O}_K$

exists and is unique up to isomorphisms ([15], 9.4.35 or [24], VII.1.3.). Over a semi-local Dedekind domain, one can define similarly the notion of (minimal) Weierstrass model ([15], 9.4.35).

The notion of Weierstrass model depends *a priori* on the origin of  $E$ . However, the next proposition says that, up to isomorphism, the choice of the origin does not matter. See also discussions in §8.

**Proposition 4.3.** *Let  $(E, e)$  be an elliptic curve over  $K$  with minimal Weierstrass model  $\mathcal{W}$  over  $\mathcal{O}_K$ .*

- (1) *Let  $q \in E(K)$  and let  $\mathcal{Z}$  be the minimal Weierstrass model of  $(E, q)$  over  $\mathcal{O}_K$ . Then there exists an isomorphism  $\mathcal{W} \simeq \mathcal{Z}$  which maps  $e$  to  $q$ .*
- (2) *Let  $N \geq 0$  and let  $\epsilon_N$  be the section of  $\mathcal{W}_N$  induced by  $e$ . Let  $\bar{q} \in \mathcal{W}_N$  be a section contained in the smooth locus. Then there exists an isomorphism (not unique)  $\mathcal{W}_N \rightarrow \mathcal{W}_N$  which maps  $\bar{q}$  to  $\epsilon_N$ .*

*Proof.* (1) Let  $t : E \rightarrow E$  be an isomorphism which maps  $e$  to  $q$ . Then  $\mathcal{Z}$  endowed with the open immersion  $j : E \xrightarrow{t} E \rightarrow \mathcal{Z}$  is a Weierstrass model  $(E, e)$ . By the uniqueness property, we get an isomorphism  $\mathcal{W} \rightarrow \mathcal{Z}$  as desired.

(2) As  $\mathcal{O}_K$  and  $\widehat{\mathcal{O}}_K$  coincide modulo  $\pi^{N+1}$ , we can suppose  $\mathcal{O}_K$  is complete. We can lift  $\bar{q}$  to a rational point  $q \in E(K)$ . Let  $t : E \rightarrow E$  be as in (1). Let  $\mathcal{E}^0$  be the identity component of the Néron model  $\mathcal{E}$  of  $E$ . It is equal to the smooth locus of  $\mathcal{W}$ . By the universal property of  $\mathcal{E}$ ,  $t$  extends to a morphism  $\mathcal{E}^0 \rightarrow \mathcal{E}$ . As  $t(e) \in \mathcal{E}^0$ ,  $t$  is actually a morphism  $\mathcal{E}^0 \rightarrow \mathcal{E}^0 \subseteq \mathcal{W}$ . As  $\mathcal{W} \setminus \mathcal{E}^0$  has codimension  $\geq 2$  in  $\mathcal{W}$ ,  $t$  extends to a finite birational morphism  $\mathcal{W} \rightarrow \mathcal{W}$ . It is an isomorphism because  $\mathcal{W}$  is normal.  $\square$

From now on  $\mathcal{W}$  will denote the **minimal Weierstrass model** of  $E$  over  $\mathcal{O}_K$ .

**Lemma 4.4.** *Fix a Weierstrass basis  $\{1, x, y\}$  of  $\mathcal{W}$ .*

- (1) *Let  $w, z \in L(3\epsilon)$ . Then  $\{1, w, z\}$  is a Weierstrass basis of  $\mathcal{W}$  if and only if  $\{1, w\}$  is a basis of  $L(2\epsilon)$ ,  $z \in L(3\epsilon) \setminus L(2\epsilon)$  and  $z^2 - w^3 \in L(5\epsilon)$ .*
- (2) *The set  $\{1, w, z\}$  is a Weierstrass basis of some Weierstrass model  $\mathcal{Z}$  if and only if  $w \in L(2\epsilon) \setminus \mathcal{O}_K$ ,  $z \in L(3\epsilon) \setminus L(2\epsilon)$ ,  $z^2 - w^3 \in L(5\epsilon)$  and  $z \in \mathcal{O}_K + \mathcal{O}_K \cdot w + \mathcal{O}_K \cdot y$ .*
- (3) *Under the above condition,  $w = u^2x + r$ ,  $z = u^3y + u^2sx + t$  for some  $u, r, s, t \in \mathcal{O}_K$  and we have  $\Delta(\mathcal{Z}) = u^{12}\Delta(\mathcal{W})$ .*

*Proof.* Let  $\{1, w, z\}$  be a Weierstrass basis of  $\mathcal{Z}$ . By [24], VII.1.3(d), there exist  $u, r, s, t \in \mathcal{O}_K$  such that

$$w = u^2x + r, \quad z = u^3y + u^2sx + t$$

and we have  $\Delta(\mathcal{Z}) = u^{12}\Delta(\mathcal{W})$ . We have  $z - sw \in \mathcal{O}_K + \mathcal{O}_K y$ . This implies (3) and the "only if" part of (1) and (2).

Conversely, let  $\{w, z\}$  satisfy the conditions of (2). Write  $w = \alpha_1x + r$ ,  $z = \alpha_3y + \alpha_4x + t$  with  $\alpha_i, r, t \in \mathcal{O}_K$ . The condition  $z^2 - w^3 \in L(5\epsilon)$  implies

that  $\alpha_1 = u^2$  and  $\alpha_3 = u^3$  where  $u = \alpha_3/\alpha_1$ . As  $u^2 \in \mathcal{O}_K$ , we have  $u \in \mathcal{O}_K$ . Since

$$u^3y + (\alpha_4/u^2)w + (t - r\alpha_4/u^2) = z \in \mathcal{O}_K + \mathcal{O}_Kw + \mathcal{O}_Ky,$$

we have  $\alpha_4 \in u^2\mathcal{O}_K$ . Formula (1.6) in [7] shows that  $\{1, w, z\}$  is a Weierstrass basis of some Weierstrass model  $\mathcal{Z}$ . If  $\{1, w\}$  is a basis of  $L(2\epsilon)$ , then  $u \in \mathcal{O}_K^*$  and  $\mathcal{Z}$  is minimal.  $\square$

Let  $L/K$  be a finite Galois extension of  $K$  with Galois group  $G$ . Let  $\mathcal{W}'$  be the minimal Weierstrass model of  $E_L$  over  $\mathcal{O}_L$  and let  $\epsilon' \subset \mathcal{W}'(\mathcal{O}_L)$  be the closure in  $\mathcal{W}'$  of the origin of  $E_L$ . As we saw before, for all  $n \geq 1$ ,  $L(n\epsilon')$  is free of rank  $n$  and  $L((n+1)\epsilon')/L(n\epsilon')$  is free of rank 1 over  $\mathcal{O}_L$ . Let  $n \geq 2$ . Since  $L(n\epsilon')^G$  is a torsion-free  $\mathcal{O}_K$ -module, it is free of rank  $n$  over  $\mathcal{O}_K$  (because on the generic fiber  $(L(n\epsilon') \otimes K)^G = L(n\epsilon) \otimes K$ ). Moreover, the quotient  $L((n+1)\epsilon')^G/(L(n\epsilon')^G)$  injects into  $L((n+1)\epsilon')/L(n\epsilon')$ , thus is free, of rank 1 (checked by  $\otimes K$ ).

**Lemma 4.5.** *The Galois group  $G$  acts on the  $\mathcal{O}_K$ -scheme  $\mathcal{W}'$  and induces a semi-linear  $G$ -action (cf. §2) on  $L(n\epsilon')$  for all  $n \in \mathbb{N}$ . Moreover, a subset  $\{1, w, z\} \subset L(3\epsilon')$  is a Weierstrass basis of some Weierstrass model of  $E$  over  $\mathcal{O}_K$  if and only if*

$$w \in L(2\epsilon')^G \setminus \mathcal{O}_K, \quad z \in L(3\epsilon')^G \setminus L(2\epsilon')^G$$

and

$$z^2 - w^3 \in L(5\epsilon'), \quad z \in \mathcal{O}_L + \mathcal{O}_Lw + \mathcal{O}_Ly'.$$

*Proof.* Let  $\{1, x', y'\}$  be a Weierstrass basis of  $\mathcal{W}'$ . The group  $G$  acts on  $E_L$  through its action on  $L$ . Let  $\sigma \in G$ . Then  $\sigma(x'), \sigma(y') \in \Gamma(E_L, \mathcal{O}_{E_L}(3o))$  define an equation of  $E_L$  with coefficients in  $\mathcal{O}_L$ . By 4.4, we have  $\sigma(x') \in L(2\epsilon')$  and  $\sigma(y') \in L(3\epsilon')$ . Therefore  $\sigma$  acts on  $\mathcal{W}'$ , hence on  $L(n\epsilon')$  for all  $n \geq 1$ . The action is semi-linear because it is on the generic fiber and  $L(n\epsilon') \subset L(n\epsilon') \otimes L$ . As the equation defined by  $w, z$  is also a Weierstrass equation of  $E_L$  over  $\mathcal{O}_L$ , the necessary part of the assertion on  $\{1, w, z\}$  results from 4.4(2). The condition is also sufficient because  $w, z$  will define a Weierstrass equation with coefficients in  $\mathcal{O}_L$ . But by the uniqueness of the coefficients (for given  $w, z$ ) over  $L$ , they all belong to  $\mathcal{O}_L \cap K = \mathcal{O}_K$ . Thus  $w, z$  define a Weierstrass equation of  $E$  over  $\mathcal{O}_K$ .  $\square$

**Theorem 4.6.** *Let  $v_L$  denote the normalized valuation on  $L$  (so  $v_L(\pi_L) = 1$ ) associated to a maximal ideal of  $\mathcal{O}_L$ . Let  $\mathcal{W}, \mathcal{W}'$  be the respective minimal Weierstrass models of  $E$  and  $E_L$ . Then*

$$0 \leq v_L(\Delta(\mathcal{W})) - v_L(\Delta(\mathcal{W}')) \leq 12(v_L(\mathfrak{D}_{L/K}) + e_{L/K} - 1).$$

*Proof.* The filtration  $\mathcal{O}_K \subseteq L(2\epsilon')^G \subseteq L(3\epsilon')^G$  has successive quotients free of rank 1 over  $\mathcal{O}_K$ . This implies the existence of a basis  $\{1, w_0, z_0\}$  of  $L(3\epsilon')^G$  over  $\mathcal{O}_K$  such that  $\{1, w_0\}$  is a basis of  $L(2\epsilon')^G$  over  $\mathcal{O}_K$ . Let  $\{1, x', y'\}$  be a Weierstrass basis of  $\mathcal{W}'$ . Then there exist  $a_1, \dots, a_5 \in \mathcal{O}_L$ , such that

$w_0 = a_1x' + a_2$ ,  $z_0 = a_3y' + a_4x' + a_5$  and  $a_1, a_3 \neq 0$ . There exist  $\alpha_1, \alpha_3 \in K^*$  such that  $\alpha_1w_0, \alpha_3z_0 \in L(3\epsilon) \otimes K$  define a Weierstrass equation of  $E$  over  $K$ . This implies that  $t := a_3^2/a_1^3 = \alpha_1^3/\alpha_3^2 \in K$ .

Now let us construct a Weierstrass model  $\mathcal{Z}$  of  $E$  over  $\mathcal{O}_K$ . If  $t \in \mathcal{O}_K$ , set

$$\beta_1 = \pi^{2n}t, \quad \beta_3 = \pi^{3n}t \in \mathcal{O}_K$$

where  $n$  is the smallest integer such that  $a_1|\pi^n$ . If  $t^{-1} \in \mathcal{O}_K$ , set

$$\beta_1 = \pi^{2m}t^{-1}, \quad \beta_3 = \pi^{3m}t^{-2} \in \mathcal{O}_K$$

where  $m$  is the smallest non-negative integer such that  $a_1|\pi^mt^{-1}$ .

Consider  $w = \beta_1w_0 \in L(2\epsilon')^G$  and  $z = \beta_3z_0 \in L(3\epsilon')^G$ . We have

$$w = \beta_1a_1x' + \beta_1a_2, \quad z = \beta_3a_3y' + \beta_3a_4x' + \beta_3a_5.$$

We can check that  $(\beta_1a_1)^3 = (\beta_3a_3)^2$ , and  $\beta_3/(\beta_1a_1) = a_1^{-1}(\pi^n t) \in \mathcal{O}_K$  if  $t \in \mathcal{O}_K$  and  $\beta_3/(\beta_1a_1) = a_1^{-1}(\pi^m t^{-1}) \in \mathcal{O}_K$  otherwise. Thus  $\beta_3a_4 \in \beta_1a_1\mathcal{O}_L$  and  $z \in \mathcal{O}_L + \mathcal{O}_Lw + \mathcal{O}_Ly'$ . By Lemma 4.5,  $\{1, w, z\}$  is a Weierstrass basis of some Weierstrass model  $\mathcal{Z}$  of  $E$  over  $\mathcal{O}_K$ . In particular  $v_K(\Delta(\mathcal{Z})) \geq v_K(\Delta(\mathcal{W}))$ .

Now let us compute  $v_L(\beta_1a_1)$ . We have

$$\beta_1a_1 = \begin{cases} (a_1^{-1}\pi^n)^2a_3^2 & \text{if } t \in \mathcal{O}_K \\ (a_1^{-1}\pi^mt^{-1})^2a_3^2 & \text{otherwise.} \end{cases}$$

By Proposition 3.3,

$$\mathfrak{D}_{L/K} \cdot L(3\epsilon') \subseteq L(3\epsilon')^G \mathcal{O}_L = \mathcal{O}_L + \mathcal{O}_Lw_0 + \mathcal{O}_Lz_0.$$

Hence  $v_L(a_3) \leq v_L(\mathfrak{D}_{L/K})$ . Therefore

$$v_L(\Delta(\mathcal{Z})) - v_L(\Delta(\mathcal{W}')) = 6v_L(\beta_1a_1) \leq 12(v_L(\mathfrak{D}_{L/K}) + e_{L/K} - 1).$$

□

**Corollary 4.7.** *Keep the notation of Theorem 4.6. Let  $\{1, x, y\}$  be a Weierstrass basis of  $\mathcal{W}$  and let  $\{1, x', y'\}$  be a Weierstrass basis of  $\mathcal{W}'$ .*

(1) *Then*

$$x = b_1x' + b_2, \quad y = b_3y' + b_4x' + b_5, \quad b_i \in \mathcal{O}_L$$

*with*

$$v_L(b_1) \leq 2(v_L(\mathfrak{D}_{L/K}) + e_{L/K} - 1), \quad v_L(b_3) \leq 3(v_L(\mathfrak{D}_{L/K}) + e_{L/K} - 1).$$

(2) *The  $\mathcal{O}_K$ -modules  $L(2\epsilon')^G/L(2\epsilon)$  and  $L(3\epsilon')^G/L(3\epsilon)$  are annihilated respectively by  $\pi^{2[v_K(\mathfrak{D}_{L/K})]+3}$  and  $\pi^{2[v_K(\mathfrak{D}_{L/K})]+4}$ .*

*Proof.* (1) As  $x \in L(2\epsilon')$  and  $y \in L(3\epsilon')$ , we can write  $x = b_1x' + b_2$ ,  $y = b_3y' + b_4x' + b_5$  for  $b_i \in \mathcal{O}_L$ . By Lemma 4.4, we have  $b_1^3 = b_3^2$  and  $v_L(\Delta(\mathcal{W})) - v_L(\Delta(\mathcal{W}')) = 6v_L(b_1)$ . The bounds on  $v_L(b_1)$  and  $v_L(b_3)$  are then a consequence of Theorem 4.6 and of the relation  $b_3^2 = b_1^3$ .

(2) Keep the notation in the proof of 4.6. As  $\beta_1w_0, \beta_3z_0 \in L(3\epsilon)$ , it is enough to bound  $v_K(\beta_1)$  and  $v_K(\beta_3)$ . The computations in the proof of Theorem 4.6 imply that  $v_L(\beta_1) \leq v_L(\beta_1a_1) \leq 2v_L(\mathfrak{D}_{L/K}) + 2e_{L/K} - 2$  and

$\beta_3 = \beta_1 a_1 \gamma_1$  with  $\gamma_1 = \pi^n/a_1$  if  $t \in \mathcal{O}_K$  and  $\gamma = (\pi^m t)/a_1$  otherwise. Hence  $v_L(\beta_3) \leq v_L(\beta_1) + e_{L/K} - 1$ . Dividing by the ramification index  $e_{L/K}$  we then get (2).  $\square$

**Corollary 4.8.** *Suppose  $E$  has good reduction over some Galois extension  $L$ . Then*

$$v_K(\Delta(\mathcal{W})) \leq [12(v_L(\mathfrak{D}_{L/K}) - 1)/e_{L/K}] + 12.$$

**Remark 4.9** If  $E$  has semi-stable reduction over  $K$ , then the formation of  $\mathcal{W}$  commutes with base changes and  $v_L(\Delta(\mathcal{W})) = v_L(\Delta(\mathcal{W}'))$ . More generally, if  $L$  contains an extension  $F/K$  such that  $E_F$  has semi-stable reduction, then  $v_L(\Delta(\mathcal{W}')) = v_L(\Delta(\mathcal{W}''))$  for the minimal Weierstrass model  $\mathcal{W}''$  of  $E_F$ .

**Remark 4.10** (*Absolute bound for the minimal discriminant*) Let  $f$  be the conductor of  $E$  and let  $m$  be the number of geometric irreducible components of the special fiber of the minimal regular model  $\mathcal{X}$  of  $E$  over  $\mathcal{O}_K$ . Then Ogg-Saito's formula ([20], Corollary 2, [25], §IV.11) is

$$v_K(\Delta(\mathcal{W})) = f + m - 1.$$

Suppose that  $E$  has potentially good reduction (equivalently,  $v_K(j(E)) \geq 0$ ). Then the Kodaira-Néron type of  $E$  is different from  $I_n^*$  if  $p \neq 2$  and we have  $m \leq 8$  by examining the list of all types. Therefore, if  $E$  acquires good reduction over some tamely ramified extension, then  $f \leq 2$  and we have  $v_K(\Delta(\mathcal{W})) \leq 10$ . Over a finite extension of  $\mathbb{Q}_p$ , by [4], Theorem 6.2  $f \leq 2 + 6v_K(2) + 3v_K(3)$ . Hence

$$v_K(\Delta(\mathcal{W})) \leq 10 + 6v_K(2) + 3v_K(3).$$

To be more precise, [4] gives a bound on the Artin conductor  $f(V, L/K)$  for any  $G$ -module  $V$  ([4], §5), and the bound on  $f$  is then deduced using the  $G$ -module of the  $\ell$ -torsions  $E[\ell]$  for a prime number  $\ell \neq p$ . Our Corollary 4.8 is of different nature because it gives a bound of  $v_K(\Delta(\mathcal{W}))$  in terms of the Artin conductor for the representation  $r_G - I_G$  (regular representation minus unit representation). It gives a better bound when  $v_L(\mathfrak{D}_{L/K})$  is small with respect to  $\max\{v_L(2), v_L(3)\}$ .

**Remark 4.11** If  $E$  has potentially multiplicative reduction, then there is no absolute bound for its minimal discriminant. However if we consider the invariant  $c_4(\mathcal{W})$ , then  $j(E) = c_4^3/\Delta$ . With similarly to Theorem 4.6, we have  $0 \leq v_L(c_4(\mathcal{W})) - v_L(c_4(\mathcal{W}')) \leq 4(v_L(\mathfrak{D}_{L/K}) + e_{L/K} - 1)$ . Hence

$$v_K(c_4(\mathcal{W})) \leq [4(v_L(\mathfrak{D}_{L/K}) - 1)/e_{L/K}] + 4$$

for any (quadratic) extension  $L/K$  such that  $E_L$  has multiplicative reduction.

**4.12 Base change conductor.** Suppose  $K$  henselian. In [6] and [5], C-L. Chai and J-K. Yu introduced the notion of base change conductor for algebraic tori and abelian varieties over  $K$ . Here we will just consider the case of elliptic curves. Consider the Néron model  $\mathcal{E}$  (resp.  $\mathcal{E}'$ ) of  $E$  (resp.

$E_L$ ) over  $\text{Spec}\mathcal{O}_K$  (resp.  $\text{Spec}\mathcal{O}_L$ ). By the universal property of the Néron model, there exists a canonical morphism  $f : \mathcal{E} \otimes_{\mathcal{O}_K} \mathcal{O}_L \rightarrow \mathcal{E}'$  which extends the isomorphism on the generic fibers. Let  $\omega_{\mathcal{E}/\mathcal{O}_K}$  (resp.  $\omega_{\mathcal{E}'/\mathcal{O}_L}$ ) be the module of the translation invariant differential forms on  $\mathcal{E}$  (resp.  $\mathcal{E}'$ ) over  $\text{Spec}\mathcal{O}_K$  (resp.  $\text{Spec}\mathcal{O}_L$ ). Let  $L/K$  be a Galois extension such that  $E_L$  has semi-stable reduction. By definition, the *base change conductor*  $c(E) \in \mathbb{Q}$  of  $E$  is the length of  $\omega_{\mathcal{E}'/\mathcal{O}_L}/f_*(\omega_{\mathcal{E}/\mathcal{O}_K} \otimes \mathcal{O}_L)$  as  $\mathcal{O}_L$ -modules divided by the ramification index  $e_{L/K}$  of  $L/K$ .

**Proposition 4.13.** *Suppose  $K$  henselian. Let  $\mathcal{W}$  be the minimal Weierstrass model of  $E$  over  $\mathcal{O}_K$ . Then the base change conductor  $c(E)$  is given by*

$$c(E) = \min\left\{\frac{1}{12}v_K(\Delta(\mathcal{W})), \frac{1}{4}v_K(c_4(\mathcal{W}))\right\}$$

*Proof.* We know that  $\omega_{\mathcal{E}/\mathcal{O}_K}$  (resp.  $\omega_{\mathcal{E}'/\mathcal{O}_L}$ ) is a free  $\mathcal{O}_K$ -module (resp.  $\mathcal{O}_L$ -module) generated by some canonical differential form  $\omega = dx/(2y + a_1x)$  (resp.  $\omega'$ ) ([15], Proposition 9.4.35). By Lemma 4.4, there exists  $u \in \mathcal{O}_L$  such that  $\omega' = u\omega$  and  $\Delta(\mathcal{W}) = u^{12}\Delta(\mathcal{W}')$ ,  $c_4(\mathcal{W}) = u^4c_4(\mathcal{W}')$ . Hence  $c(E) = v_L(u)/e_{L/K}$ . If  $E$  has potentially good reduction, then  $v_L(\Delta(\mathcal{W}')) = 0$ ,  $c(E) = v_K(\Delta(\mathcal{W}))/12$  and

$$\frac{1}{4}v_K(c_4(\mathcal{W})) - \frac{1}{12}v_K(\Delta(\mathcal{W})) = \frac{1}{12}v_K(j) \geq 0.$$

Similarly, if  $E$  has potentially multiplicative reduction, then  $v_L(c_4(\mathcal{W}')) = 0$ ,  $c(E) = v_K(c_4(\mathcal{W}))/4$  and  $v_K(c_4(\mathcal{W}))/4 < v_K(\Delta(\mathcal{W}))$  because  $v_K(j) < 0$ .  $\square$

**Corollary 4.14.** *Let  $L/K$  be a finite Galois extension such that  $E_L$  has semi-stable reduction. Then*

$$c(E) < v_K(\mathfrak{D}_{L/K}) + 1.$$

*In particular, if  $\text{char}(K) = 0$ , then*

$$c(E) < 24v_K(p)/(p-1) + 1.$$

*Proof.* The first part comes from Corollary 4.8 and Remark 4.11. For the second, note that  $E$  has semi-stable reduction over an extension  $L/K$  of degree dividing 24 (see the end of the proof of Theorem 5.9) and then use Remark 3.10.  $\square$

## 5. CONGRUENCES OF MINIMAL WEIERSTRASS MODELS

From now on, we will suppose that  $K$  has *perfect residue field*. This hypothesis is used only in Lemma 5.1.

For any scheme  $\mathcal{Z}$  over  $\mathcal{O}_K$  (including  $\mathcal{O}_L$ -schemes), recall that

$$\mathcal{Z}_N := \mathcal{Z} \times_{\text{Spec}\mathcal{O}_K} \text{Spec}(\mathcal{O}_K/\pi^{N+1}\mathcal{O}_K)$$

for any non-negative integer  $N$ . Similarly, recall that for any  $\mathcal{O}_K$  or  $\mathcal{O}_L$ -module  $M$ , we denote

$$M_N = M/\pi^{N+1}M.$$



We keep the notation of §4. In particular,  $\mathcal{W}$  and  $\mathcal{W}'$  are the respective minimal Weierstrass model of  $E$  and  $E_L$  over  $\mathcal{O}_K$  and  $\mathcal{O}_L$ , and  $\epsilon'$  is the closure in  $\mathcal{W}'$  of the origin of  $E_L$ . We will also work with another discrete valuation field  $K_o$  with perfect residue field, a Galois extension  $L_o/K_o$  of group  $G$  and an elliptic curve  $E_o$  over  $K_o$ . We will denote analogous construction by the same notation with a subscript  $o$ . We will say  $\mathcal{W}_N$  is *determined by the  $G$ -action on  $\mathcal{W}'_m$*  (or *by  $(\mathcal{W}'_m, G)$  for short*) for some  $m \geq N$  if the existence of compatible  $G$ -equivariant isomorphisms:

$$(\text{Iso}_m) \quad \begin{cases} \mathcal{O}_{K,m} \simeq \mathcal{O}_{K_o,m}, \\ \theta_m : \mathcal{O}_{L,m} \simeq \mathcal{O}_{L_o,m}, \\ \mathcal{W}'_m \simeq \mathcal{W}'_{o,m}, \quad \epsilon'_m \mapsto \epsilon'_{o,m} \end{cases}$$

implies  $\mathcal{W}_N \simeq \mathcal{W}_{o,N}$ . Let us stress that  $\mathcal{W}'_m \rightarrow \mathcal{W}'_{o,m}$  is supposed to map  $\epsilon'_m$  to  $\epsilon'_{o,m}$  (the Weierstrass models should be regarded as *pointed schemes*). The aim of this section is to show that  $\mathcal{W}_N$  is determined by  $(\mathcal{W}'_m, G)$  when  $m \gg 0$  (Theorem 5.6).

**Lemma 5.1.** *Let  $N > v_K(\mathfrak{D}_{L/K}) - 1$ . If  $\mathcal{O}_{L,N} \simeq \mathcal{O}_{L_o,N}$  as  $G$ -modules, then  $v_{L_o}(\mathfrak{D}_{L_o/K_o}) = v_L(\mathfrak{D}_{L/K})$  and  $e_{L/K} = e_{L_o/K_o}$ .*

*Proof.* The maximal ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  of  $\mathcal{O}_L$  correspond to the maximal ideals of the semi-local ring  $\mathcal{O}_{L,N}$ . Hence there is a one-one correspondence between the maximal ideals of  $\mathcal{O}_L$  and that of  $\mathcal{O}_{L_o}$ . We have

$$\mathfrak{D}_{L/K} \hat{\mathcal{O}}_{L,\mathfrak{p}_i} = \mathfrak{D}_{\hat{\mathcal{O}}_{L,\mathfrak{p}_i}/\hat{\mathcal{O}}_K}$$

It is therefore enough to deal with the case when  $K$  is complete.

The isomorphism  $\mathcal{O}_L/\pi\mathcal{O}_L \simeq \mathcal{O}_{L_o}/\pi_o\mathcal{O}_{L_o}$  implies the equality of ramification indexes  $e_{L/K} = e_{L_o/K_o}$ . Let  $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_r = \{1\}$  be the ramification filtration of  $G$  acting on  $\mathcal{O}_L$  (with  $G_{r-1}$  non-trivial). Then

$$v_L(\mathfrak{D}_{L/K}) = \left( \sum_{i \geq 0} (|G_i| - 1) \right) \geq r$$

([23], IV.1, Proposition 4<sup>2</sup>). As  $v_L(\sigma(\pi_L) - \pi_L) \leq r$  for all  $\sigma \in G \setminus \{1\}$ , the same property holds for  $\pi_{L_o}$  thanks to the isomorphism

$$\theta_N : \mathcal{O}_L/\pi_L^{(N+1)e_{L/K}} \mathcal{O}_L \simeq \mathcal{O}_{L_o}/\pi_{L_o}^{(N+1)e_{L/K}} \mathcal{O}_{L_o}$$

with  $(N+1)e_{L/K} > v_L(\mathfrak{D}_{L/K}) \geq r$ . Thus the ramification filtration of  $G$  acting on  $L_o$  is the same as that of  $G$  acting on  $L$ . Hence  $v_L(\mathfrak{D}_{L/K}) = v_{L_o}(\mathfrak{D}_{L_o/K_o})$ .  $\square$

**Lemma 5.2.** *Let  $N \geq 0$  and let  $n \geq 1$ . Then  $\epsilon'_N$  is the support of an effective Cartier divisor on  $\mathcal{W}'_N$ ,  $\mathcal{O}_{\mathcal{W}'}(3\epsilon'_N)$  is very ample and the canonical map*

$$\Gamma(\mathcal{W}', \mathcal{O}_{\mathcal{W}'}(n\epsilon'))_N \rightarrow \Gamma(\mathcal{W}'_N, \mathcal{O}_{\mathcal{W}'}(n\epsilon'_N))$$

*is an isomorphism.*

<sup>2</sup>Here the hypothesis  $k$  perfect is used. We don't know whether it is really necessary.

*Proof.* The first assertion comes from the fact that  $\epsilon'$  is an effective relative Cartier divisor on  $\mathcal{W}' \rightarrow \text{Spec } \mathcal{O}_L$ . The remaining part is contained in [7], §1.  $\square$

Fix  $N \geq 0$  and let  $m \geq N$ . Suppose we are given isomorphisms  $(\text{Iso}_m)$  as above. Then they induce canonically isomorphisms  $(\text{Iso}_i)$  for all integers  $0 \leq i \leq m$ . The isomorphisms  $\mathcal{W}'_i \rightarrow \mathcal{W}'_{o,i}$  ( $0 \leq i \leq m$ ) induce  $G$ -invariant isomorphisms

$$\varphi_i : L(6\epsilon'_o)_i \simeq L(6\epsilon')_i, \quad i \leq m$$

which respect the filtration by poles orders and are compatible with the multiplications  $L(n\epsilon'_o)_i \times L(r\epsilon'_o)_i \rightarrow L((n+r)\epsilon'_o)_i$ .

For any element  $z \in M$  in some  $\mathcal{O}_K$ -module, we denote by  $\bar{z}$  its image in  $M_i$  if no confusion is possible.

**Lemma 5.3.** *Let  $\{1, x'_o, y'_o\}$  be a Weierstrass basis of  $\mathcal{W}'_o$ . Then the subset  $\{1, \varphi_m(\bar{x}'_o), \varphi_m(\bar{y}'_o)\} \subset L(3\epsilon')_m$  lifts to a Weierstrass basis of  $\mathcal{W}'$ .*

*Proof.* Lift arbitrarily  $\varphi_m(\bar{x}'_o), \varphi_m(\bar{y}'_o)$  to  $w' \in L(2\epsilon')$  and  $z' \in L(3\epsilon')$ . There exist  $\lambda_i \in \mathcal{O}_L$  such that  $w' = \lambda_1 x' + \lambda_2$ ,  $z' = \lambda_3 y' + \lambda_4 w' + \lambda_5$  (recall that  $\{1, x', y'\}$  is a Weierstrass basis of  $\mathcal{W}'$ ). As  $\varphi_m$  is an isomorphism,  $\lambda_1, \lambda_3 \in \mathcal{O}_L^*$ . The relation  $(y'_o)^2 - (x'_o)^3 \in L(5\epsilon'_o)$  implies that  $\lambda_3^2 - \lambda_1^3 = 0$  in  $\mathcal{O}_{L,m}$ . Therefore  $\lambda := \lambda_3^2/\lambda_1^3 \in 1 + \pi^{m+1}\mathcal{O}_L$ . Replacing  $w'$  (resp.  $z'$ ) by  $\lambda w'$  (resp.  $\lambda z'$ ), we find new liftings  $w, z$  such that  $z^2 - w^3 \in L(5\epsilon')$  and  $\{1, w, z\}$  is a basis of  $L(3\epsilon')$ . This implies that  $\{1, w, z\}$  is a Weierstrass basis of  $\mathcal{W}'$ .  $\square$

The next lemma is used in Example 2.1 and in Proposition 7.7.

**Lemma 5.4.** *Let  $N \geq 0$ , let  $\mathcal{W}, \mathcal{W}_o$  be respective Weierstrass models of  $E, E_o$  over  $\mathcal{O}_K$  and let  $\{1, x, y\}, \{1, x_o, y_o\}$  be corresponding Weierstrass basis. Suppose there exists an isomorphism  $\varphi_N : \mathcal{W}_N \simeq \mathcal{W}_{o,N}$ . Then the following properties are true:*

(1) *there exists  $u, s, r \in \mathcal{O}_{K,N}$  such that  $u \in \mathcal{O}_{K,N}^*$  and*

$$\varphi_N(\bar{x}_o) = u^2 \bar{x} + r, \quad \varphi_N(\bar{y}_o) = u^3 \bar{y} + u^2 s \bar{x} + t.$$

(2) *If  $N \geq 5$ , then  $\mathcal{W}$  is minimal if and only if  $\mathcal{W}_o$  is minimal.*

*Proof.* (1) is an immediate consequence of Lemma 5.3 and of Lemma 4.4(3).

(2) First the minimality of  $\mathcal{W}$  can be checked over the strict henselization of  $\mathcal{O}_K$ . As  $k$  is perfect, we can suppose  $k$  is algebraically closed. By Tate's algorithm [26], §7-8,  $\mathcal{W}$  is not minimal if and only if there exists  $r, s, t \in \mathcal{O}_K$  such that  $v(a'_i) \geq i$ . This condition is checked modulo  $\pi^6$ , so in  $\mathcal{W}_5$ .  $\square$

**Lemma 5.5.** *Let*

$$0 \rightarrow M \rightarrow H \rightarrow T \rightarrow 0$$

*be an exact sequence of  $\mathcal{O}_K$ -modules such that  $\pi^r T = 0$  for some  $r \geq 1$ . Then for all  $m \geq r$ ,*

$$\ker(M_m \rightarrow H_m) \subseteq \ker(M_m \rightarrow M_{m-r}).$$

*Proof.* The kernel  $\ker(M_m \rightarrow H_m)$  is isomorphic by the Snake Lemma to  $T[\pi^{m+1}]$ , kernel of  $[(\pi^{m+1})_T]$  (the multiplication-by- $\pi^{m+1}$  map on  $T$ ), and the canonical surjection  $M_m \rightarrow M_{m-r}$  induces on  $T[\pi^{m+1}] \rightarrow T[\pi^{m+1-r}]$  the map  $[(\pi^r)_T]$ . This implies the lemma.  $\square$

**Theorem 5.6.** *Let  $N \geq 0$ . If*

$$m \geq N + 12[v_K(\mathfrak{D}_{L/K})] + 19,$$

*then  $\mathcal{W}_N$  is determined by the  $G$ -action on  $\mathcal{W}'_m$ .*

*Proof.* By hypothesis, we have isomorphisms  $(\text{Iso}_m)$  (hence  $(\text{Iso}_i)$  for all  $i \leq m$ ). Denote by  $\rho_i$  the canonical maps  $L(3\epsilon)_i \rightarrow (L(3\epsilon')^G)_i$  and by  $\rho_{o,i}$  the analogue maps for  $E_o$ . We have a commutative diagram

$$\begin{array}{ccccccc} L(3\epsilon_o)_m & \xrightarrow{\rho_{o,m}} & (L(3\epsilon'_o)^G)_m & \hookrightarrow & (L(3\epsilon'_o)_m)^G & \hookrightarrow & L(3\epsilon'_o)_m \\ & & & & \downarrow \varphi_m & & \downarrow \varphi_m \\ L(3\epsilon)_m & \xrightarrow{\rho_m} & (L(3\epsilon')^G)_m & \hookrightarrow & (L(3\epsilon')_m)^G & \hookrightarrow & L(3\epsilon')_m \end{array}$$

where the vertical arrows are isomorphisms. We want to complete this diagram with an isomorphism  $L(3\epsilon_o)_{m_2} \simeq L(3\epsilon)_{m_2}$  for some  $m_2 \leq m$  and sending a Weierstrass basis to a Weierstrass basis. Let  $\{1, x_o, y_o\}$  be a Weierstrass basis of  $\mathcal{W}_o$ .

**Step 1.** Let  $\mathfrak{D} = \mathfrak{D}_{L/K}$ . Let  $m_1 = m - 2[v_K(\mathfrak{D})]$ . We first construct images of  $x_o, y_o$  in  $(L(3\epsilon')^G)_{m_1}$ . According to Proposition 3.9, the above commutative diagram induces a new commutative diagram at level  $m_1$  (we omit  $L(3\epsilon'_o)_{m_1}$  and  $L(3\epsilon')_{m_1}$ ) with isomorphic arrows

$$\begin{array}{ccccccc} L(3\epsilon_o)_{m_1} & \xrightarrow{\rho_{o,m_1}} & (L(3\epsilon'_o)^G)_{m_1} & \hookrightarrow & (L(3\epsilon'_o)_{m_1})^G & & \\ & & \downarrow \varphi_{m_1} & & \downarrow \varphi_{m_1} & & \\ L(3\epsilon)_{m_1} & \xrightarrow{\rho_{m_1}} & (L(3\epsilon')^G)_{m_1} & \hookrightarrow & (L(3\epsilon')_{m_1})^G & & \end{array}$$

Let  $w \in L(2\epsilon')^G, z \in L(3\epsilon')^G$  be liftings of  $\varphi_{m_1}(\bar{x}_o)$  and  $\varphi_{m_1}(\bar{y}_o)$ .

**Step 2.** Now we modify  $w, z$  to  $x, y$  so that  $\{1, x, y\}$  is a Weierstrass basis of a Weierstrass model of  $E$  over  $\mathcal{O}_K$ . We can write

$$x_o = b_{o,1}x'_o + b_{o,2}, \quad y_o = b_{o,3}y'_o + b_{o,4}x'_o + b_{o,5}, \quad b_{o,i} \in \mathcal{O}_{L_o}$$

where  $\{1, x'_o, y'_o\}$  is a Weierstrass basis of  $\mathcal{W}'$ . By Corollary 4.7(1) and Lemma 5.1, and by Lemma 4.4(3), we have

$$v_{L_o}(b_{o,1}) \leq 2(v_{L_o}(\mathfrak{D}_{L_o/K_o}) + e_{L_o/K_o} - 1) \leq m_1, \quad v_{L_o}(b_{o,1}) \leq v_{L_o}(b_{o,4}).$$

Let  $\{1, x', y'\}$  be a Weierstrass basis of  $\mathcal{W}'$  whose image in  $L(3\epsilon')_m$  is equal to  $\{1, \varphi_m(\bar{x}'_o), \varphi_m(\bar{y}'_o)\}$  (Lemma 5.3). Then

$$(3) \quad w = c_1x' + c_2, \quad z = c_3y' + c_4x' + c_5, \quad c_i \in \mathcal{O}_L.$$

For all  $i \leq 5$ ,  $\bar{c}_i = \theta_{m_1}(\bar{b}_{o,i}) \in \mathcal{O}_{L,m_1}$ . Therefore

$$(4) \quad v_L(c_1) \leq 2(v_L(\mathfrak{D}) + e_{L/K} - 1) \leq m_1, \quad v_L(c_1) \leq v_L(c_4).$$

We have

$$\bar{c}_3^2 - \bar{c}_1^3 = \theta_{m_1}(\bar{b}_{o,3})^2 - \theta_{m_1}(\bar{b}_{o,1})^3 = 0 \in \mathcal{O}_{L,m_1}$$

(Lemma 4.4(3)). Writing  $w, z$  in a Weierstrass basis of  $E$  (with coefficients in  $K$ ), we see that  $\lambda := c_3^2/c_1^3 \in K$ . Moreover, the inequality on  $v_L(c_1)$  implies that  $v_L(c_1^3)/e < 6[v_K(\mathfrak{D})] + 12$ , hence

$$\lambda \in 1 + \pi^{m_1+1-[6v_K(\mathfrak{D})]-11}\mathcal{O}_K.$$

Let  $x = \lambda w$  and  $y = \lambda z$  and let  $m_2 = m_1 - 6[v_K(\mathfrak{D})] - 11$ . Then  $y^2 - x^3 \in L(5\epsilon')$  and  $x, y \in L(3\epsilon')^G$  coincide with  $w, z$  in  $(L(3\epsilon')^G)_{m_2}$ . Multiplying Equation (3) above by  $\lambda$ , using the second inequality of Equation (4) and Lemma 4.5, we see that  $\{1, x, y\}$  is a Weierstrass basis of a Weierstrass model  $\mathcal{Z}$  of  $E$  over  $\mathcal{O}_K$ . This implies that  $x \in L(2\epsilon), y \in L(3\epsilon)$ .

**Step 3.** Let us show that  $\{1, x, y\}$  is a Weierstrass basis of  $\mathcal{W}$ . The above construction shows that we have a canonical commutative diagram

$$\begin{array}{ccccc} (L(3\epsilon'_o)^G)_{m_2} & \xrightarrow{\varphi_{m_2}} & (L(3\epsilon')^G)_{m_2} & \xrightarrow{\varphi_{m_2}^{-1}} & (L(3\epsilon'_o)^G)_{m_2} \\ \uparrow & & \uparrow & & \uparrow \\ \text{Im}(\rho_{o,m_2}) & \longrightarrow & \text{Im}(\rho_{m_2}) & \longrightarrow & \text{Im}(\rho_{o,m_2}) \\ \uparrow \rho_{m_2} & & \uparrow \rho_{m_2} & & \uparrow \rho_{m_2} \\ L(3\epsilon_o)_{m_2} & & L(3\epsilon)_{m_2} & & L(3\epsilon_o)_{m_2} \end{array}$$

which implies that  $\varphi_{m_2}(\text{Im}(\rho_{o,m_2})) = \text{Im}(\rho_{m_2})$ . Thus  $\{1, x, y\}$  generate  $L(3\epsilon)$  in  $(L(3\epsilon')^G)_{m_2}$ . As  $m_2 \geq 2[v_K(\mathfrak{D})] + 4$ , it follows from Corollary 4.7(2) that

$$\ker(L(3\epsilon) \rightarrow (L(3\epsilon')^G)_{m_2}) \subseteq \pi^{m_2+1}L(3\epsilon')^G = \pi(\pi^{m_2}L(3\epsilon')^G) \subseteq \pi L(3\epsilon).$$

By Nakayama's lemma,  $\{1, x, y\}$  generate, hence is a basis of,  $L(3\epsilon)$ . Therefore  $\{1, x, y\}$  is a Weierstrass basis of  $\mathcal{W}$ .

**Last step:** Let's show  $\mathcal{W}_N \simeq \mathcal{W}_{o,N}$ . Let

$$y_o^2 + (a_{o,1}x_o + a_{o,3})y_o = x_o^3 + a_{o,2}x_o^2 + a_{o,4}x_o + a_{o,6}$$

be the equation of  $\mathcal{W}_o$ . Let  $a_i \in \mathcal{O}_K$  be such that  $\bar{a}_i = \varphi_{m_2}(\bar{a}_{o,i})$ . Then

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$$

holds in  $(L(6\epsilon')^G)_{m_2}$ . By Lemma 5.5 and Corollary 4.7(2), the same relation holds in  $L(6\epsilon)_{m_3}$ , where  $m_3 = m_2 - (4[v_K(\mathfrak{D})] + 8)$ . Therefore  $\mathcal{W}_{m_3} \simeq \mathcal{W}_{o,m_3}$ . As  $m_3 \geq N$ , we have  $\mathcal{W}_N \simeq \mathcal{W}_{o,N}$ .  $\square$

**Remark 5.7** The bound on  $m$  in 5.6 is not optimal. When  $L/K$  is unramified, we can take  $m = N$ .

**Proposition 5.8.** *Suppose  $E$  has semi-stable reduction over  $\mathcal{O}_K$ . Then for any  $N \geq 0$ ,  $\mathcal{W}_N$  is determined by  $(\mathcal{W}'_m, G)$  if  $m \geq 2[v_K(\mathfrak{D}_{L/K})] + N$ . In particular,  $\mathcal{W}_N$  is determined by  $(\mathcal{W}'_N, G)$  if  $L/K$  is tamely ramified.*

*Proof.* Suppose we are given a system of isomorphisms  $(\text{Iso}_m)$ . Then the special fiber of  $\mathcal{W}_o$  is semi-stable because it is isomorphic to the special fiber of  $\mathcal{W}$ . Hence  $\mathcal{W}_o$  is semi-stable. The minimal Weierstrass model  $\mathcal{W}$  commutes with base changes by Dedekind domains when  $E$  has semi-stable reduction. Therefore  $\mathcal{W}' = \mathcal{W}_{\mathcal{O}_L}$ ,  $\mathcal{W}'_o = (\mathcal{W}_o)_{\mathcal{O}_{L_o}}$ , and

$$H^1(G, L(6\epsilon')) = H^1(G, L(6\epsilon) \otimes \mathcal{O}_L) = H^1(G, \mathcal{O}_L) \otimes L(6\epsilon)$$

is killed by  $\pi^{2[v_K(\mathfrak{D}_{L/K})]}$  (Proposition 3.7). Let  $m_1 = m - 2[v_K(\mathfrak{D}_{L/K})] \geq N$ . As in the proof Theorem 5.6, we have a commutative diagram

$$\begin{array}{ccc} L(3\epsilon_o)_{m_1} = (L(3\epsilon'_o)^G)_{m_1} & \hookrightarrow & (L(3\epsilon'_o)_{m_1})^G \\ \downarrow \varphi_{m_1} & & \downarrow \varphi_{m_1} \\ L(3\epsilon)_{m_1} = (L(3\epsilon')^G)_{m_1} & \hookrightarrow & (L(3\epsilon')_{m_1})^G \end{array}$$

As in Lemma 5.3, the image of a Weierstrass basis  $\{1, x_o, y_o\}$  of  $\mathcal{W}_o$  by  $\varphi_{m_1}$  lifts to a Weierstrass basis  $\{1, x, y\}$  of  $\mathcal{W}$ . Therefore  $\mathcal{W}_{m_1} \simeq \mathcal{W}_{o, m_1}$ .  $\square$

**Theorem 5.9.** *Suppose  $K$  is henselian,  $\text{char}(K) = 0$ , and the residue field is algebraically closed of characteristic  $p > 0$ . Then there exists a positive integer  $l$ , depending only on the absolute ramification index  $v_K(p)$ , such that for any elliptic curve  $E$  over  $K$ , and for  $L/K$  the minimal extension such that  $E_L$  has semi-stable reduction,  $\mathcal{W}_N$  is determined by the  $G$ -action on  $\mathcal{W}'_{N+l}$  for any  $N \geq 0$ .*

*Proof.* First, the field extension  $L/K$  is Galois ([8], théorème 5.15). It is well known that  $[L : K]$  divides 24: if  $v_K(j(E)) < 0$ , then  $|G| = 1$  or 2. Otherwise, the curve  $E$  has potentially good reduction  $\mathcal{X}'_{s'}$ , and we have an injection  $G \hookrightarrow \text{Aut}(\mathcal{X}'_{s'})$  ([8], Lemma 5.16). The latter has order dividing 24 ([24], III.10, Theorem 10.1), so  $|G|$  divides 24. The corollary then follows from Remark 3.10 and Theorem 5.6.  $\square$

## 6. FROM WEIERSTRASS MODELS TO REGULAR MODELS

Recall that the residue field of  $K$  is perfect (to use Kodaira-Néron's classification, and Ogg-Saito's formula). The minimal regular model  $\mathcal{X}$  is the minimal desingularization of  $\mathcal{W}$  ([15], Corollary 9.4.37). The models we considered are *pointed* with the Zariski closure of the neutral element of  $E$ . In this section, we will prove that  $\mathcal{W}_{N+c}$  determines  $\mathcal{X}_N$  for an explicit constant  $c$  depending on the type of  $E$  (Corollary 6.7). This will follow from some general results on relation between a  $\mathcal{O}_K$ -scheme of finite type and its blowups along a closed points (Theorem 6.4).

First we show that the second order deformation determines the singular locus.

**Lemma 6.1.** *Let  $\mathcal{Y}$  be a scheme flat and locally of finite type over  $\mathcal{O}_K$ , of pure relative dimension  $d$  and with regular generic fiber. Let  $y_0 \in \mathcal{Y}_0$  be a closed point. Then  $\mathcal{Y}$  is regular at  $y_0$  if and only if either  $\dim T_{\mathcal{Y}_0, y_0} = d$ , or  $\dim T_{\mathcal{Y}_0, y_0} = d + 1$  and  $\pi \in \mathfrak{m}_{\mathcal{Y}, y_0}^2$ . In particular, the singular locus of  $\mathcal{Y}$  is determined by  $\mathcal{Y}_1$ .*

*Proof.* The condition  $\dim T_{\mathcal{Y}_0, y_0} = d$  means  $\mathcal{Y}_0$  (hence  $\mathcal{Y}$ ) is regular at  $y_0$ . We have an exact sequence of  $k(y_0)$ -vector spaces

$$0 \rightarrow \pi \mathcal{O}_{\mathcal{Y}, y_0} / (\pi \mathcal{O}_{\mathcal{Y}, y_0} \cap \mathfrak{m}_{\mathcal{Y}, y_0}^2) \rightarrow \mathfrak{m}_{\mathcal{Y}, y_0} / \mathfrak{m}_{\mathcal{Y}, y_0}^2 \rightarrow \mathfrak{m}_{\mathcal{Y}_0, y_0} / \mathfrak{m}_{\mathcal{Y}_0, y_0}^2 \rightarrow 0.$$

So the second condition is equivalent to  $\mathcal{Y}$  regular and  $\mathcal{Y}_0$  singular at  $y_0$ . The condition  $\pi \in \mathfrak{m}_{\mathcal{Y}, y_0}^2$  is equivalent to  $\pi \in \mathfrak{m}_{\mathcal{Y}, y_0}^2 \bmod \pi^2$ . So the singular locus of  $\mathcal{Y}$  is determined by  $\mathcal{Y}_1$ .  $\square$

**Notation** For any  $\mathcal{O}_K$ -algebra  $A$  and for any  $n \geq 0$ , we denote by

$$A[\pi^n] = \{x \in A \mid \pi^n x = 0\}, \quad A_{\text{tors}} = \cup_{n \geq 1} A[\pi^n].$$

By convention  $\pi^0 = 1$  and  $A[\pi^0] = 0$ . We use similar notation when  $A$  is replaced with a sheaf of  $\mathcal{O}_K$ -algebras.

**Lemma 6.2.** *Let  $U'$  be a noetherian  $\mathcal{O}_K$ -scheme and let  $U = V(\mathcal{J})$  be a closed subscheme of  $U'$ , flat over  $\mathcal{O}_K$  and containing  $U'_K$ . Then*

- (1)  $\mathcal{J} = \mathcal{O}_{U', \text{tors}} = \mathcal{O}_{U'}[\pi^c]$  for some  $c \geq 0$ .
- (2) *The composition of the closed immersions  $U_N \rightarrow U'_N \rightarrow U'_{N+c}$  induces an isomorphism*

$$U_N \simeq V(\mathcal{O}_{U'_{N+c}}[\pi^c]).$$

*Proof.* (1) As  $U \supseteq U'_K$ , we have  $\mathcal{J}_K = 0$ , hence  $\mathcal{J} \subseteq \mathcal{O}_{U', \text{tors}}$ . As  $\mathcal{J}$  is coherent, we can find a  $c \geq 0$  such that  $\pi^c \mathcal{J} = 0$ , thus  $\mathcal{J} \subseteq \mathcal{O}_{U'}[\pi^c]$ . Conversely,  $\mathcal{O}_{U'}[\pi^c] \subseteq \mathcal{O}_{U', \text{tors}} \subseteq \mathcal{J}$  because  $\mathcal{O}_U$  is torsion free over  $\mathcal{O}_K$ .

(2) The kernel of  $\mathcal{O}_{U'_{N+c}} \rightarrow \mathcal{O}_{U_N}$  is the image of  $\mathcal{J} + \pi^{N+1} \mathcal{O}_{U'}$  in  $\mathcal{O}_{U'_{N+c}}$ , and we check easily that this image is equal to  $\mathcal{O}_{U'_{N+c}}[\pi^c]$ .  $\square$

Next we will give a bound for  $c$  in a specific situation.

**Proposition 6.3.** *Let  $\mathcal{Z}$  be a noetherian regular scheme, let  $\rho: \tilde{\mathcal{Z}} \rightarrow \mathcal{Z}$  be the blowing-up of  $\mathcal{Z}$  along a closed point  $q$ , let  $\mathcal{Y}$  be an integral hypersurface in  $\mathcal{Z}$  (thus an effective Cartier divisor) passing through  $q$  and let  $\tilde{\mathcal{Y}}$  be the strict transform of  $\mathcal{Y}$  (which is isomorphic to the blowup of  $\mathcal{Y}$  along  $q$ ). Then the following properties hold:*

- (1)  *$\tilde{\mathcal{Y}}$  is an integral hypersurface in  $\tilde{\mathcal{Z}}$  and, if  $\rho^* \mathcal{Y}$  denotes the pullback of  $\mathcal{Y}$  as Cartier divisor,*

$$\rho^* \mathcal{Y} = \tilde{\mathcal{Y}} + \mu_q(\mathcal{Y})E$$

*where  $\mu_q(\mathcal{Y})$  is the multiplicity of  $\mathcal{Y}$  at  $q$  and  $E$  is the prime exceptional divisor  $\rho^{-1}(q)$ .*

- (2) *Let  $\tilde{q} \in \tilde{\mathcal{Y}}$  be a closed point lying over  $q$ . Then  $\mu_{\tilde{q}}(\tilde{\mathcal{Y}}) \leq \mu_q(\mathcal{Y})$ .*

- (3) Suppose further that  $\mathcal{Z}$  is an  $\mathcal{O}_K$ -scheme,  $\mathcal{Y}$  is flat and  $q$  belongs to the closed fiber of  $\mathcal{Y}$ . Let  $r_E \geq 1$  be the multiplicity of  $E$  in the special fiber of  $\tilde{\mathcal{Z}}$  (equal to the multiplicity at  $q$  of the special fiber of  $\mathcal{Z}$ ) and let  $c = \lceil \mu_q(\mathcal{Y})/r_E \rceil$  be the smallest integer bigger or equal to  $\mu_q(\mathcal{Y})/r_E$ . Then

$$\mathcal{O}_{\rho^*\mathcal{Y}, \text{tors}} = \mathcal{O}_{\rho^*\mathcal{Y}}[\pi^c] \neq \mathcal{O}_{\rho^*\mathcal{Y}}[\pi^{c-1}].$$

*Proof.* (1) is certainly well known. We provide a proof here for completeness. Since  $\tilde{\mathcal{Z}}$  is a blowup of a regular scheme along a regular closed subscheme,  $\tilde{\mathcal{Z}}$  is also regular ([15], 8.1.19). Then  $\rho^*\mathcal{Y}$  is an effective Cartier divisor with support in  $\tilde{\mathcal{Y}} \cup E$  and we can write  $\rho^*\mathcal{Y} = \tilde{\mathcal{Y}} + rE$  for some positive integer  $r$ . As the computation of  $r$  and  $\mu_q$  are local on  $\mathcal{Z}$ , we can replace  $\mathcal{Z}$  with  $\text{Spec} \mathcal{O}_{\mathcal{Z}, q}$  and suppose  $\mathcal{Z}$  is local. Write  $C = \mathcal{O}_{\mathcal{Z}, q}$  with maximal ideal  $\mathfrak{m}$ . Choose a system of coordinates  $t_0, \dots, t_d$  of  $C$ . Then  $\tilde{\mathcal{Z}}$  is covered by the affine open subsets  $U_i =: \text{Spec}(C[t_0/t_i, \dots, t_r/t_i])$ ,  $0 \leq i \leq d$ . Let  $f \in \mathfrak{m}$  be a local equation of  $\mathcal{Y}$ . Write

$$f = P(t_0, \dots, t_d) + f_{\mu+1}, \quad f_{\mu+1} \in \mathfrak{m}^{\mu+1}$$

where  $P$  is homogeneous of degree  $\mu = \mu_q(\mathcal{Y})$  with coefficients in  $C^*$  and  $P \notin \mathfrak{m}^{\mu+1}$ . Here we use the fact that  $\text{grad}_{\mathfrak{m}}(C) \simeq \text{Sym}(\mathfrak{m}/\mathfrak{m}^2)$ . On  $U_0$  (and similarly on each  $U_i$ ), we have

$$f = t_0^\mu P(1, u_1, \dots, u_d) + t_0^{\mu+1} g_0, \quad u_i := t_i/t_0, \quad g_0 \in \mathcal{O}_{\tilde{\mathcal{Z}}}(U_0).$$

A local equation of  $E$  at its generic point is  $t_0$  and that of  $\rho^*\mathcal{Y}$  is  $f$ . As  $u_1, \dots, u_d$  is a system of coordinates of  $E$ , we have  $f \in t_0^\mu \mathcal{O}_{\tilde{\mathcal{Z}}}(U_0) \setminus t_0^{\mu+1} \mathcal{O}_{\tilde{\mathcal{Z}}}(U_0)$  and  $r = \mu$ .

(2) This is a particular case of [2], Chap. I, Theorem 0.

(3) The decomposition  $\rho^*\mathcal{Y} = \tilde{\mathcal{Y}} + \mu E$  gives an exact sequence

$$0 \rightarrow \mathcal{O}_{\tilde{\mathcal{Z}}}(-\tilde{\mathcal{Y}})|_{\mu E} = \mathcal{O}_{\tilde{\mathcal{Z}}}(-\tilde{\mathcal{Y}})/\mathcal{O}_{\tilde{\mathcal{Z}}}(-\tilde{\mathcal{Y}} - \mu E) \rightarrow \mathcal{O}_{\rho^*\mathcal{Y}} \rightarrow \mathcal{O}_{\tilde{\mathcal{Y}}} \rightarrow 0.$$

As  $\tilde{\mathcal{Y}}$  is flat over  $\mathcal{O}_K$ , and  $\mathcal{O}_{\tilde{\mathcal{Z}}}(-\tilde{\mathcal{Y}})|_{\mu E}$  is of torsion (namely killed by  $\pi^c$  because, by the definition of  $c$ ,  $\mu E$  is contained in  $c$  times the closed fiber of  $\tilde{\mathcal{Z}}$ ), we have

$$\mathcal{O}_{\rho^*\mathcal{Y}, \text{tors}} = \mathcal{O}_{\tilde{\mathcal{Z}}}(-\tilde{\mathcal{Y}})|_{\mu E} = \mathcal{O}_{\rho^*\mathcal{Y}}[\pi^c]$$

and  $\pi^{c-1} \mathcal{O}_{\rho^*\mathcal{Y}} \neq 0$ . □

**Theorem 6.4.** *Let  $\mathcal{Y}$  be a flat  $\mathcal{O}_K$ -scheme of finite type and let  $q$  be a closed point of  $\mathcal{Y}$  contained in the closed fiber. Suppose further that  $\mathcal{Y}$  is locally at  $q$  a hypersurface in a regular  $\mathcal{O}_K$ -scheme of finite type. Let  $\tilde{\mathcal{Y}} \rightarrow \mathcal{Y}$  be the blowing-up along  $q$ , and let  $\ell \geq c$  (the constant defined as in 6.3 (3)). Then  $\mathcal{Y}_{N+\ell}$  determines  $(\tilde{\mathcal{Y}})_N$  for all  $N \geq 0$ .*

More precisely, suppose we have a discrete valuation ring  $\mathcal{O}_{K_o}$  and  $(\mathcal{Y}_o, q_o)$  over  $\mathcal{O}_{K_o}$  with similary properties and  $q_o$  and the constant  $c_o \leq \ell$ . If we have an isomorphism  $\phi_{N+\ell} : \mathcal{O}_{K, N+\ell} \rightarrow \mathcal{O}_{K_o, N+\ell}$  and a compatible isomorphism

$$\mathcal{Y}_{N+\ell} \simeq \mathcal{Y}_{o, N+\ell}$$

for some  $N \geq 0$ , then we have an isomorphism

$$(\tilde{\mathcal{Y}})_N \simeq (\tilde{\mathcal{Y}}_o)_N$$

compatible with the isomorphism  $\mathcal{O}_{K,N} \simeq \mathcal{O}_{K_o,N}$  induced by  $\phi_{N+\ell}$ .

*Proof.* We can suppose  $\mathcal{Y}$  is singular at  $q$  (then  $\mathcal{Y}_o$  is also singular at  $q_o$  by Lemma 6.1). Then  $\dim_{k(q)} T_{\mathcal{Y},q} = d+1$  if  $d = \dim \mathcal{O}_{\mathcal{Y},q}$ . Let  $f_0, \dots, f_d$  be a minimal system of generators of  $\mathfrak{m}_q \mathcal{O}_{\mathcal{Y},q}$ , let  $\mathcal{Y}'$  be the glueing of  $\mathcal{Y} \setminus \{q\}$  and of  $\text{Proj} \mathcal{O}_{\mathcal{Y},q}[T_0, \dots, T_d]/(f_i T_j - f_j T_i)_{0 \leq i, j \leq d}$ . Then  $\tilde{\mathcal{Y}}$  is a flat closed subscheme of  $\mathcal{Y}'$  with generic fiber equal to that of  $\mathcal{Y}'$ . Therefore  $\tilde{\mathcal{Y}} = V(\mathcal{O}_{\mathcal{Y}', \text{tors}})$ . Using a lifting in  $\mathcal{O}_{\mathcal{Y}_o, q_o}$  of the images of the  $f_i$ 's in  $\mathcal{O}_{(\mathcal{Y}_o)_{N+\ell}, q_o}$ , we define  $\mathcal{Y}'_o$  and clearly we have an isomorphism

$$\mathcal{Y}'_{N+\ell} \simeq \mathcal{Y}'_{o, N+\ell}$$

extending the isomorphism  $\mathcal{Y}_{N+\ell} \simeq \mathcal{Y}_{o, N+\ell}$ . So, by Lemma 6.2, to show that  $(\tilde{\mathcal{Y}})_N \simeq (\tilde{\mathcal{Y}}_o)_N$ , it is enough to show that  $\pi^\ell \mathcal{O}_{\mathcal{Y}', \text{tors}} = 0$ . This property is local on  $\mathcal{Y}$ . As it trivially holds outside of  $q$ , it is enough to work with a small open neighborhood of  $q$  in  $\mathcal{Y}$ .

Write locally  $\mathcal{Y} = \text{Spec} C/(f)$  with  $(C, \mathfrak{m}_C)$  regular. Lift  $f_0, \dots, f_d$  to  $t_0, \dots, t_d \in C$ . Because  $\mathfrak{m}_C/\mathfrak{m}_C^2 \rightarrow \mathfrak{m}_q/\mathfrak{m}_q^2$  is surjective and both vector spaces have the same dimension over  $k(q)$ , this is an isomorphism and  $t_0, \dots, t_d$  is a system of coordinates of  $C$ . Consider

$$B = C[T_0, \dots, T_d]/(f, t_i T_j - t_j T_i)_{i,j}.$$

Let  $\rho : \widetilde{\text{Spec} C} \rightarrow \text{Spec} C$  be the blowing-up of  $\text{Spec} C$  along  $q$ . Then  $\mathcal{Y}' = \text{Proj} B = \rho^* \mathcal{Y}$  and Proposition 6.3 shows that  $\pi^\ell \mathcal{O}_{\mathcal{Y}', \text{tors}} = 0$  and we are done.  $\square$

**Remark 6.5** Note that one can't determine  $(\tilde{\mathcal{Y}})_N$  with a blowup of  $\mathcal{Y}_{N+\ell}$  because the latter process produces a scheme which is birational to  $\mathcal{Y}_{N+\ell}$ , while  $(\tilde{\mathcal{Y}})_N$  has more irreducible components than  $\mathcal{Y}_{N+\ell}$ .

**Remark 6.6** Let  $f : \mathcal{X} \rightarrow \mathcal{W}$  be the desingularization morphism of  $\mathcal{W}$ . If  $\mathcal{W}$  is singular, the pre-image of the singular point of  $\mathcal{W}$  consists in  $(-2)$ -curves. It is well known that such singular points are rational singularities (one can apply [1], Theorem 3, because the fundamental cycle  $Z$  satisfies  $2p_a(Z) - 2 = Z^2 < 0$ ). Let  $\mathcal{Z} \rightarrow \mathcal{W}$  be the blowing-up of the singular point of  $\mathcal{W}$ . Then  $\mathcal{Z}$  is normal ([14], Proposition 8.1) and its singular points are rational singularities ([14], Proposition 1.2). Therefore the morphism  $f : \mathcal{X} \rightarrow \mathcal{W}$  consists in successive blowing-ups

$$\mathcal{X} = \mathcal{W}^{(t)} \rightarrow \mathcal{W}^{(t-1)} \rightarrow \dots \mathcal{W}^{(1)} \rightarrow \mathcal{W}^{(0)} = \mathcal{W}$$

along (reduced and discrete) singular loci.

**Corollary 6.7.** *Let  $\mathcal{W}$  be the minimal Weierstrass model of  $E$ . Let  $\mathcal{X}$  be the minimal regular model of  $E$  over  $\mathcal{O}_K$  and let  $t$  be the number of blowing-ups defined as above. Then*



- (1)  $\mathcal{W}_{N+\ell}$  determines  $\mathcal{X}_N$  if  $\ell \geq 2t + 1$ .
- (2)  $t + 1$  is bounded by the number of irreducible components of  $\mathcal{X}_0$ . In particular,  $t \leq 8$  if the Kodaira type of  $E$  is different from  $I_n$  and  $I_n^*$ .
- (3) Let  $\Delta$  be the minimal discriminant of  $E$ . Then  $t \leq v_K(\Delta) - 1$ , except when  $E$  has good reduction.

*Proof.* (1) If  $\mathcal{W}$  is regular (i.e.  $E$  has type  $I_0$ ,  $I_1$  or  $II$ ), then  $\mathcal{X} = \mathcal{W}$  and there is nothing to prove. So we suppose  $\mathcal{W}$  is singular. The scheme  $\mathcal{W}$  is embedded in  $\mathcal{Z} = \mathbb{P}_{O_K}^2$  as a cubic. Around the singular point  $q$ ,  $\mathcal{W}$  is defined by a regular function  $y^2 + (a_1x + a_3)y - (x^3 + \dots) \in \mathfrak{m}_{\mathcal{Z},q}^2 \setminus \mathfrak{m}_{\mathcal{Z},q}^3$ . So  $\mu_q(\mathcal{W}) = 2$ . Let  $\ell \geq 1$  be any positive integer. Applying Theorem 6.4, we see that  $\mathcal{W}_{N+\ell}$  determines  $\mathcal{W}_{N+\ell-2}^{(1)}$ . As  $\mathcal{W}^{(1)}$  is embedded (and has codimension 1) in  $\tilde{\mathcal{Z}}$  which is regular, Proposition 6.3 and Theorem 6.4 imply that  $\mathcal{W}_{N+\ell-2}^{(1)}$  determines  $\mathcal{W}_{N+\ell-4}^{(2)}$ . Repeating the same arguments we see that  $\mathcal{W}_{N+\ell}$  determines  $\mathcal{W}_{N+\ell-2t}^{(t)}$ . This means that  $\mathcal{W}_{N+\ell} \simeq \mathcal{W}_{o,N+\ell}$  implies that  $\mathcal{W}_{N+\ell-2t}^{(t)} \simeq \mathcal{W}_{o,N+\ell-2t}^{(t)}$ . Note that by Lemma 6.1, the isomorphism  $\mathcal{W}_{N+\ell-2i}^{(i)} \simeq \mathcal{W}_{o,N+\ell-2i}^{(i)}$  maps the singular locus of  $\mathcal{W}^{(i)}$  to that of  $\mathcal{W}_o^{(i)}$ , so  $\mathcal{W}_o^{(i+1)} \rightarrow \mathcal{W}_o^{(i)}$  is the blowing-up of the singular locus of  $\mathcal{W}^{(i)}$ .

Now taking  $\ell = 2t$  might not be enough (when  $N = 0$ ) because we don't know whether  $\mathcal{W}_o^{(t)}$  is the minimal regular model of  $E_o$ . We have to go one step further. Namely if  $\mathcal{W}_{N+2t+1} \simeq \mathcal{W}_{o,N+2t+1}$ , then  $\mathcal{W}_{N+1}^{(t)} \simeq \mathcal{W}_{o,N+1}^{(t)}$ . By Lemma 6.1, we know that  $\mathcal{W}_o^{(t)}$  is regular and  $\mathcal{W}_o^{(t-1)}$  is singular. Therefore,  $t = t_o$  and  $\mathcal{W}_o^{(t_o)} = \mathcal{X}_o$ .

(2) As each blowing-up  $\mathcal{W}^{(i+1)} \rightarrow \mathcal{W}^{(i)}$  introduces at least one irreducible component, we see that  $t + 1$  is at most equal to the number of irreducible components of  $\mathcal{X}_0$ .

(3) This is a direct consequence of (2) and Ogg-Saito's formula.  $\square$

**Remark 6.8** Tate's algorithm shows that  $\mathcal{W}_6$  determines whether  $E$  has type  $I_n$  (for some indeterminate  $n \geq 0$ ),  $II$ ,  $III$ ,  $IV$ ,  $II^*$ ,  $III^*$ ,  $IV^*$  or  $I_n^*$  (for some indeterminate  $n$ ). But  $\mathcal{W}_6$  can't determine the value of  $n$  in general in the case  $I_n$  or  $I_n^*$ .

Below is a table with more precise value of  $t$ , the number of blowing-ups necessary to solve the singularities of  $\mathcal{W}$ .

type of $E$	$I_0, I_1, II$	$III, IV$	$II^*$	$III^*$	$IV^*$	$I_n$	$I_n^*$
value of $t$	0	1	$\leq 8$	$\leq 7$	4	$\lfloor n/2 \rfloor$	$\leq n + 4$

**Example 6.9** Suppose  $\text{char}(k) \neq 2$ . Let  $n \geq 1$  and consider the elliptic curves

$$E : y^2 = (x^2 + \pi^{2n+1})(x + 1), \quad E_o : y^2 = (x^2 + \pi^{2n+2})(x + 1).$$

We have  $\mathcal{W}_{2n} \simeq \mathcal{W}_{o,2n}$ , but  $\mathcal{X}_0 \not\simeq \mathcal{X}_{o,0}$ . Here  $t = n$  but  $t_o = n + 1$ .

## 7. CONGRUENCES OF MINIMAL REGULAR MODELS

In this section we prove the main theorem of this paper (Theorem 7.3). The idea is to show that  $\mathcal{X}'_{N+\ell_1+\ell_2}$  determines  $\mathcal{W}'_{N+\ell_1+\ell_2}$  which determines  $\mathcal{W}_{N+\ell_1}$  for some  $\ell_2$  and finally that  $\mathcal{W}_{N+\ell_1}$  determines  $\mathcal{X}_N$  for some  $\ell_1$ .

As  $\mathcal{W}$  is regular in a neighborhood of  $\epsilon$ ,  $\mathcal{X} \rightarrow \mathcal{W}$  is an isomorphism above a neighborhood of  $\epsilon$ . So denote again by  $\epsilon$  the closure in  $\mathcal{X}$  of the neutral element of  $E$ . The effective Cartier divisor  $\epsilon$  on  $\mathcal{X}$  is ample on the generic fiber and meets in the special fiber  $\mathcal{X}_0$  only in the strict transform  $\widetilde{\mathcal{W}}_0$  of the irreducible component of  $\mathcal{W}_0$ . Therefore  $\mathcal{W}$  is the contraction in  $\mathcal{X}$  of the components different from  $\widetilde{\mathcal{W}}_0$ . By construction, there is a canonical isomorphism

$$(5) \quad \mathcal{W} \simeq \text{Proj}(\oplus_{n \geq 0} H^0(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(n\epsilon)))$$

(see [3], Theorem 6.7/1).

**Lemma 7.1.** *Let  $N \geq 0$ . Then*

$$\mathcal{W}_N \simeq \text{Proj}(\oplus_{n \geq 0} H^0(\mathcal{X}_N, \mathcal{O}_{\mathcal{X}}(n\epsilon_N)))$$

*Proof.* We have to show that the canonical map

$$H^0(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(n\epsilon))_N \rightarrow H^0(\mathcal{X}_N, \mathcal{O}_{\mathcal{X}}(n\epsilon)_N)$$

is an isomorphism for all  $n \geq 0$ . Considering the exact sequence

$$0 \longrightarrow \mathcal{O}_{\mathcal{X}}(n\epsilon) \xrightarrow{\cdot \pi^{N+1}} \mathcal{O}_{\mathcal{X}}(n\epsilon) \longrightarrow \mathcal{O}_{\mathcal{X}}(n\epsilon_N) \longrightarrow 0,$$

we only have to show that  $H^1(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(n\epsilon))$  is torsion-free for all  $n \geq 0$ , or that

$$(6) \quad H^1(\mathcal{X}, \mathcal{O}_{\mathcal{X}}(n\epsilon))_0 \rightarrow H^1(\mathcal{X}_0, \mathcal{O}_{\mathcal{X}}(n\epsilon_0))$$

is surjective for all  $n \geq 0$  ([15], Theorem 5.3.20). As the dualizing sheaf  $\omega_{\mathcal{X}/\mathcal{O}_K}$  is trivial ([15], Exercise 9.4.16), we have

$$H^1(\mathcal{X}_0, \mathcal{O}_{\mathcal{X}}(n\epsilon_0)) \simeq H^0(\mathcal{X}_0, \mathcal{O}_{\mathcal{X}}(-n\epsilon_0)).$$

On the other hand  $H^0(\mathcal{X}_0, \mathcal{O}_{\mathcal{X}_0}) = k$  ([15], Corollary 9.1.24), the sheaf of ideals  $\mathcal{O}_{\mathcal{X}}(-n\epsilon_0)$  has no nontrivial section for all  $n \geq 1$ . Hence (6) is surjective for all  $n \geq 0$ .  $\square$

As in the Section 5,  $L/K$  is a finite Galois extension of Galois group  $G$ .

**Proposition 7.2.** *Let  $\mathcal{W}'$ ,  $\mathcal{X}'$  be the (pointed) minimal Weierstrass (resp. minimal regular) model of  $E_L$  over  $\mathcal{O}_L$ . Let  $N \geq 0$ . Then  $(\mathcal{W}'_N, G)$  is determined by  $(\mathcal{X}'_N, G)$ .*

*Proof.* It is enough to apply the isomorphism (5) and the previous lemma to the models  $\mathcal{W}'$  and  $\mathcal{X}'$  of  $E_L$ . Note that the isomorphism of 7.1 is compatible with the action of  $G$  because  $\epsilon$  is invariant by  $G$ .  $\square$

**Theorem 7.3.** *Let  $K$  be a discrete valuation field with perfect residue field. Let  $E$  be an elliptic curve over  $K$  of minimal discriminant  $\Delta$ . Let  $L/K$  be Galois extension of group  $G$ , of different  $\mathfrak{D}_{L/K}$ . Then for any  $N \geq 0$ , the scheme  $\mathcal{X}_N$  is determined by  $(\mathcal{X}'_{N+\ell}, G)$ , where*

$$\ell = 2v_K(\Delta) + 12[v_K(\mathfrak{D}_{L/K})] + 18.$$

*Proof.* By Proposition 7.2,  $(\mathcal{X}'_{N+\ell}, G)$  determines  $(\mathcal{W}'_{N+\ell}, G)$ . Theorem 5.6 says that the latter determines  $\mathcal{W}_{N+2v_K(\Delta)-1}$ . Finally Corollary 6.7 implies that  $\mathcal{X}_N$  is determined by the previous data.  $\square$

**Corollary 7.4.** *Suppose  $K$  is strictly henselian of mixed characteristics  $(0, p)$ . Let  $L/K$  be the minimal extension such that  $E_L$  has semi-stable reduction. Then the special fiber  $\mathcal{X}_0$  is determined by the  $G$ -action on  $\mathcal{X}'_{\ell_0}$  where  $\ell_0$  depends only on the absolute ramification index  $v_K(p)$  of  $K$ .*

*Proof.* If  $E$  has potentially multiplicative reduction, D. Lorenzini ([17], Theorem 2.8) showed that  $[L : K] \leq 2$ ,  $E$  has reduction type  $I_{n+4s}^*$  where  $n = -v_K(j(E)) > 0$  and  $s = v_L(\mathfrak{D}_{L/K}) - 1 \geq 0$ . The curve of type  $I_r^*$  is unique up to isomorphisms for each  $r > 0$  ([19], Theorem 5.18). Hence, using Lemma 5.1,  $\mathcal{X}_0$  is determined by  $\mathcal{X}'_{\ell_0}$  with  $\ell_0 = v_L(\mathfrak{D}_{L/K}) \leq 4v_K(p)/(p-1)$  (Remark 3.10).

If  $E$  has potentially good reduction, then  $v_K(\Delta) \leq 12(v_K(\mathfrak{D}_{L/K}) + 1)$  with  $[L : K]$  dividing 24, hence  $v_K(\mathfrak{D}_{L/K}) \leq 24v_K(p)/(p-1)$ . Then we conclude with Theorem 7.3.  $\square$

Next we give some inverse results of Theorem 5.6 and Theorem 7.3.

**Proposition 7.5.** *Let  $N \geq v_K(\Delta)$ . Then  $\mathcal{W}_N$  determines  $(\mathcal{W}'_N, G)$  for any finite Galois extension  $L/K$ .*

*Proof.* Let  $K_o, E_o$  and  $L_o/K_o$  be as at the beginning of §5 and suppose we have isomorphisms

$$\mathcal{O}_{K,N} \simeq \mathcal{O}_{K_o,N}, \quad \mathcal{W}_N \rightarrow \mathcal{W}_{o,N}, \quad \theta_N : \mathcal{O}_{L,N} \simeq \mathcal{O}_{L_o,N},$$

the last one being  $G$ -equivariant. We have to find a  $G$ -equivariant isomorphism  $\mathcal{W}'_N \rightarrow \mathcal{W}'_{o,N}$ .

Let  $\{1, x, y\}$  (resp.  $\{1, x', y'\}$ ) be a Weierstrass basis of  $\mathcal{W}$  (resp. of  $\mathcal{W}'$ ). By Lemma 4.4, we have a change of coordinates of  $E_L$ :

$$x = u^2 x' + r, \quad y = u^3 y' + u^2 s x' + t, \quad u, r, s, t \in \mathcal{O}_L.$$

Let  $\phi_N : L(6\epsilon)_N \simeq L(6\epsilon_o)_N$  be the isomorphism induced by  $\mathcal{W}_{o,N} \simeq \mathcal{W}_N$ . Let  $\{1, x_o, y_o\}$  be a Weierstrass basis of  $\mathcal{W}_o$  lifting the image by  $\phi_N$  of the class of  $\{1, x, y\}$  in  $L(6\epsilon)_N$ . Let  $u_o, r_o, s_o, t_o \in \mathcal{O}_{L_o}$  be liftings of the images by  $\theta_N$  of the classes  $\bar{u}, \bar{r}, \bar{s}, \bar{t} \in \mathcal{O}_{L,N}$ . Let

$$x'_o = (x_o - r_o)/u_o^2, \quad y'_o = (y_o - u_o^2 s_o x'_o - t_o)/u_o^3 \in L(6\epsilon'_o) \otimes L_o.$$

We claim that  $\{1, x'_o, y'_o\}$  is a Weierstrass basis of  $\mathcal{W}'_o$ . First, the fact that  $\{1, x, y\}$  defines a Weierstrass model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

over  $\mathcal{O}_L$  implies that

$$u \mid a_1 + 2s, \quad u^2 \mid a_2 - sa_1 + 3r - s^2, \dots,$$

and

$$u^6 \mid a_6 + ra_4 + ra_r^3 - ta_3 - t^2 - rta_1$$

(see [7], page 57, (1.6)). As

$$6v_L(u) = (v_L(\Delta) - v_L(\Delta'))/2 \leq v_L(\Delta)/2 \leq v_L(\pi^N),$$

the above divisibility relations hold in  $L(6\epsilon'_o)$ . Therefore  $\{1, x'_o, y'_o\}$  is a Weierstrass basis of some Weierstrass model over  $\mathcal{O}_{L_o}$ . In particular

$$v_L(\Delta') = v_L(\Delta) - 12v_L(u) = v_{L_o}(\Delta_o) - 12v_{L_o}(u_0) \geq v_L(\Delta'_o).$$

But by symmetry,  $v_L(\Delta'_o) \geq v_L(\Delta')$ , so the equality holds and the Weierstrass model associated to  $\{1, x'_o, y'_o\}$  is minimal over  $\mathcal{O}_{L_o}$ .

As the change of variables from  $\{1, x, y\}$  to  $\{1, x', y'\}$  and from  $\{1, x_o, y_o\}$  to  $\{1, x'_o, y'_o\}$  are given the same relations modulo  $\pi^{N+1}$  (up to  $\theta_N$ ), and  $\{1, x, y\}$ ,  $\{1, x_o, y_o\}$  define the same equation up to  $\mathcal{O}_{K,N} \simeq \mathcal{O}_{K_o,N}$ , we have an isomorphism  $\mathcal{W}'_N \rightarrow \mathcal{W}'_{o,N}$  corresponding to  $\bar{x}' \rightarrow \bar{x}'_o$  and  $\bar{y}' \rightarrow \bar{y}'_o$ .  $\square$

**Proposition 7.6.** *Let  $\Delta$  be the minimal discriminant of  $E$ . Then for any  $N \geq 0$ ,  $(\mathcal{X}'_N, G)$  is determined by  $\mathcal{X}_{N+2v_L(\Delta)-1}$ .*

*Proof.* Let  $\ell = 2v_K(\Delta) - 1$ . First, by Proposition 7.2 (for  $L = K$ ),  $\mathcal{X}_{N+\ell}$  determines  $\mathcal{W}_{N+\ell}$ . Second,  $\mathcal{W}_{N+\ell}$  determines  $(\mathcal{W}'_{N+\ell}, G)$  by Proposition 7.5. Finally, the latter determines  $(\mathcal{X}'_N, G)$  by similar arguments than Corollary 6.7 (note that  $v_L(\Delta)$  is bigger or equal to the  $v_L$  valuation of the minimal discriminant of  $E_L$ ).  $\square$

**Proposition 7.7.** *Suppose  $\text{char}(K) = p > 0$  with perfect residue field  $k$ . Let  $N \geq 0$ . Then there exists a discrete valuation field  $K_o$  of characteristic 0, with residue field equal to  $k$ , and an elliptic curve  $E_o$  over  $K_o$  such that*

$$\mathcal{O}_{K_o,N} \simeq \mathcal{O}_{K,N}, \quad \mathcal{W}_{o,N} \simeq \mathcal{W}_N, \quad \mathcal{X}_{o,N} \simeq \mathcal{X}_N.$$

*Proof.* Let  $n \geq \max\{5, N + 2v_K(\Delta) - 1\}$  so that  $\mathcal{X}_N$  is determined by  $\mathcal{W}_n$  (Corollary 6.7). Let  $\mathcal{O}_{K_o} = W(k)[t]/(t^{n+1} - p)$  with uniformizing element  $\pi_o = t$ . Then  $\mathcal{O}_{K_o,n} \simeq \mathcal{O}_{K,n}$ . Lifting  $\mathcal{W}_n$  to a Weierstrass equation  $\mathcal{W}_o$  over  $\mathcal{O}_{K_o}$ , then we have  $v_{K_o}(\Delta_o) = v_K(\Delta)$  and  $\mathcal{W}_o$  is minimal by Lemma 5.4(2). By construction,  $\mathcal{W}_n \simeq \mathcal{W}_{o,n}$  (hence  $\mathcal{W}_N \simeq \mathcal{W}_{o,N}$ ). Again by Corollary 6.7, we have an isomorphism  $\mathcal{X}_N \simeq \mathcal{X}_{o,N}$ .  $\square$

## 8. LIFTING EQUIVARIANT INFINITESIMAL SECTIONS

In our settings, Weierstrass models come with a fixed section. But in Proposition 4.3, we saw that up to isomorphisms, the choice of a section does not really matter. We can wonder whether in Theorem 5.6 we can dismiss the given section of  $\mathcal{W}'_m$ . Note that, at least in our proof, we use the fact that this section of  $\mathcal{W}'_m$  is  $G$ -equivariant and even more, that it extends to a section of  $\mathcal{W}'$  over  $\mathcal{O}_L$  induced by a rational point in  $E(K)$ . Now suppose we are given  $(\text{Iso}_m)$  as at the beginning of §5 but without the condition that the isomorphism  $\mathcal{W}'_m \simeq \mathcal{W}'_{o,m}$  maps  $\epsilon'_m$  to  $\epsilon'_{o,m}$ . The image of  $\epsilon'_m$  is a  $G$ -equivariant section of  $\mathcal{W}'_{o,m}$  contained in the smooth locus of  $\mathcal{W}'_{o,m}$ . If for some  $m_1 \leq m$ , the image of  $\epsilon'_{m_1}$  in  $\mathcal{W}'_{o,m_1}$  extends to a section  $Q$  of  $\mathcal{W}'_o$  induced by a rational point of  $q \in E_o(K_o)$  (equivalently,  $Q$  is a  $G$ -equivariant section of  $\mathcal{W}'_o$ ), then by Proposition 4.3 we have a  $G$ -equivariant isomorphism  $\mathcal{W}'_{m_1} \simeq \mathcal{W}'_{o,m_1}$  which maps  $\epsilon'_{m_1}$  to  $\epsilon'_{o,m_1}$  and we can apply Theorem 5.6 with  $m_1$  instead of  $m$ .

Let  $S$  be a scheme. Let  $f : X' \rightarrow S'$  be a morphism of  $S$ -schemes and let  $H$  be a group acting on the  $S$ -schemes  $X', S'$  compatibly with  $f$  (in other words,  $f$  is  $H$ -equivariant). Then  $H$  acts on the set of sections  $X'(S')$  in the following way: for any section  $\rho : S' \rightarrow X'$  and for any  $\sigma \in H$ , we put  $\sigma \star \rho = \sigma \circ \rho \circ \sigma^{-1} \in X'(S')$ . A section  $\rho$  is said  *$H$ -equivariant* if  $\sigma \star \rho = \rho$  for all  $\sigma \in H$ . The set of  $H$ -equivariant sections will be denoted by  $X'(S')^H$ . The above question is to study the image of the canonical map

$$\mathcal{W}'(\mathcal{O}_L)^G \rightarrow \mathcal{W}'(\mathcal{O}_L/\pi^{m+1}\mathcal{O}_L)^G.$$

Suppose from now on that  $S' \rightarrow S$  is finite and locally free and  $X' \rightarrow S'$  is quasi-projective. Then the Weil restriction  $R_{S'/S}X'$  exists ([3], Theorem 7.6/4) over  $S$  and is endowed with a canonical action of  $H$ . Moreover, for any  $S$ -scheme  $T$ , letting  $H$  act trivially on  $T$  and denoting  $Y = R_{S'/S}X'$ ,  $X'(S' \times_S T)^H$  is canonically isomorphic to  $Y(T)^H$ . Suppose further that  $H$  is finite. Let  $Y^H$  be the scheme of fixed points under  $H$  (see e.g. [10], §3). Then by definition  $Y(T)^H = Y^H(T)$ .

Let  $S = \text{Spec } \mathcal{O}_K$ ,  $S' = \text{Spec } \mathcal{O}_L$ ,  $S_m = \text{Spec } (\mathcal{O}_K/\pi^{m+1}\mathcal{O}_K)$  and  $S'_m = S' \times_S S_m$ .

**Proposition 8.1.** *Let  $\mathcal{Z}'$  be a flat quasi-projective scheme over  $S'$  endowed with an equivariant action of  $G = \text{Gal}(L/K)$ . Then the following properties hold.*

- (1) *Let  $\mathcal{Z} = \mathcal{Z}'/G$ . Then the canonical map  $\mathcal{Z}(S) \rightarrow \mathcal{Z}'(S')^G$  is bijective.*
- (2) *Suppose  $S' \rightarrow S$  is étale. Then the canonical morphism  $\mathcal{Z}' \rightarrow \mathcal{Z} \times_S S'$  is an isomorphism and the canonical morphism  $\mathcal{Z} \rightarrow (R_{S'/S}\mathcal{Z}')^G$  is an isomorphism.*
- (3) *Suppose that  $K$  is henselian,  $\mathcal{Z}'$  is smooth over  $S'$  and  $L/K$  is tamely ramified. Then the canonical map*

$$\mathcal{Z}'(S')^G \rightarrow \mathcal{Z}'(S'_m)^G$$

is surjective for all  $m \geq 0$ .

- (4) Suppose that  $K$  is henselian and that  $\mathcal{Z}'_L$  is smooth over  $L$ . Then there exist  $m_0, r_0 \geq 0$  such that for all  $m \geq m_0$ , and for any  $t_m \in \mathcal{Z}'(S'_m)^G$ , the image of  $t_m$  in  $\mathcal{Z}'(S'_{m-r_0})^G$  lifts to a section in  $\mathcal{Z}'(S')^G$ .

*Proof.* (1) First notice that the quotient  $\mathcal{Z}'/G$  exists because  $\mathcal{Z}'$  is quasi-projective over  $\mathcal{O}_L$ . The canonical morphism  $\mathcal{Z}'_L \rightarrow (\mathcal{Z}_K)_L$  is an isomorphism by Lemma 3.2. The canonical map

$$\mathcal{Z}'(\mathcal{O}_L)^G \rightarrow \mathcal{Z}(\mathcal{O}_K) \subseteq \mathcal{Z}_K(K)$$

is injective. Conversely, any section in  $\mathcal{Z}(\mathcal{O}_K)$  induces a rational point in  $\mathcal{Z}_K(K) = \mathcal{Z}'_L(L)^G \subseteq \mathcal{Z}'_L(L)$ . The valuative criterion of properness for  $\mathcal{Z}' \rightarrow \mathcal{Z}$  implies that the point in  $\mathcal{Z}'_L(L)$  we obtain actually belongs to  $\mathcal{Z}'(\mathcal{O}_L) \cap \mathcal{Z}'_L(L)^G = \mathcal{Z}'(\mathcal{O}_L)^G$ . Therefore  $\mathcal{Z}'(\mathcal{O}_L)^G \rightarrow \mathcal{Z}(\mathcal{O}_K)$  is surjective.

(2) The canonical morphism  $\mathcal{Z}' \rightarrow \mathcal{Z} \times_S S'$  is an isomorphism by Proposition 3.3. For any  $\mathcal{O}_K$ -module  $M$  with trivial action of  $G$ , the canonical map  $M \rightarrow (M \otimes_{\mathcal{O}_K} \mathcal{O}_L)^G$  is an isomorphism (use a normal basis of  $\mathcal{O}_L/\mathcal{O}_K$ ). For any  $S$ -scheme  $T$ , the canonical map

$$\mathcal{Z}(T) \rightarrow R_{S'/S} \mathcal{Z}'(T)^G = (\mathcal{Z}'(T \times_S S'))^G = (\mathcal{Z}(T \times_S S'))^G = \mathcal{Z}(T)$$

is bijective. So  $\mathcal{Z} \rightarrow (R_{S'/S} \mathcal{Z}')^G$  is an isomorphism.

(3) Let  $\mathcal{Y} = R_{S'/S} \mathcal{Z}'$ . We saw above that  $\mathcal{Z}'(S')^G \rightarrow \mathcal{Z}'(S'_m)^G$  can be identified with the canonical map

$$\mathcal{Y}^G(S) \rightarrow \mathcal{Y}^G(S_m).$$

Let  $I \subset G$  be the inertia group, let  $L_1 = L^I$ ,  $H = G/I$  and let  $S^t = S'/I$ . Denote by  $\mathcal{Z}^t = R_{S'/S^t} \mathcal{Z}'$ . It is smooth over  $S^t$  ([3], Proposition 7.6/5) as well as  $\mathcal{Z}_1 := (\mathcal{Z}^t)^I$  ([10], Proposition 3.4). Let  $T$  be an  $S$ -scheme with trivial action of  $G$ . Then

$$\mathcal{Z}'(T \times_S S')^G = (\mathcal{Z}'(T \times_S S')^I)^H = (\mathcal{Z}_1(T \times_S S^t))^H.$$

Let  $\mathcal{Z}_2 = \mathcal{Z}_1/H$ . By (2),  $\mathcal{Z}_2$  is smooth over  $S$  and  $(\mathcal{Z}_1(T \times_S S^t))^H = \mathcal{Z}_2(T)$ . Thus  $\mathcal{Z}'(T \times_S S')^G = \mathcal{Z}_2(T)$ . As  $\mathcal{O}_K$  is henselian and  $\mathcal{Z}_2$  is smooth,  $\mathcal{Z}_2(S) \rightarrow \mathcal{Z}_2(S_m)$  is surjective and (3) is proved.

(4) Applying (2) to  $\text{Spec} L \rightarrow \text{Spec} K$ , we see that  $\mathcal{Z}_K$  is smooth over  $K$  and  $(\mathcal{Y}^G)_K = (\mathcal{Y}_K)^G = \mathcal{Z}_K$ . Our statement then results from Elkik's approximation theorem ([11], Corollaire 1, page 567) and the identity  $\mathcal{Y}^G(T) = \mathcal{Z}'(T \times_S S')^G$  for all  $S$ -schemes  $T$ .  $\square$

**Remark 8.2** Keep the notation of Proposition 8.1.

- (1) If  $K$  is henselian,  $L/K$  is tamely ramified and  $\mathcal{Z}'$  is smooth, it is probably true that the canonical map

$$\mathcal{Z}'(\mathcal{O}_L)^G \rightarrow \mathcal{Z}'(\text{Spec}(\mathcal{O}_L/\pi_L^{m+1}\mathcal{O}_L))^G$$

is surjective for all  $m \geq 0$ . Note that the right-hand side is not  $\mathcal{Z}'(S'_m)^G$ .

- (2) The constants  $m_0, r_0$  in 8.1(4) depend on the scheme  $\mathcal{Z}'$ . When the latter is smooth over  $S'$ , it is probably true that one can find bounds  $m_0, r_0$  depending only on  $v_K(\mathfrak{D}_{L/K})$ .

Next we give in Proposition 8.4 a more precise statement than in 8.1(4) for abelian varieties. The next lemma should be well known but we were unable to find a proper reference.

**Lemma 8.3.** *Suppose  $K$  is complete of characteristic zero. Let  $A$  be an abelian variety over  $L$  of dimension  $d$ , let  $\mathcal{A}'$  be the Néron model of  $A_L$  over  $\mathcal{O}_L$  and let  $\widehat{\mathcal{A}'}$  be the formal group over  $\mathcal{O}_L$  attached to  $\mathcal{A}'$ .*

- (1) *The formal logarithm*

$$\log_{\mathcal{A}'} : \widehat{\mathcal{A}'}(\pi_L \mathcal{O}_L) \rightarrow H^0(A_L, \Omega_{A_L/L}^1)^\vee$$

*is  $G$ -equivariant.*

- (2) *For all  $n > v_L(p)/(p-1)$  ( $n > 0$  if  $p = 0$ ),  $\log_{\mathcal{A}'}$  induces a group isomorphism between  $\widehat{\mathcal{A}'}(\pi_L^n \mathcal{O}_L)$  and a sub- $\mathcal{O}_L$ -module of  $H^0(A_L, \Omega_{A_L/L}^1)^\vee$ .*

*Proof.* (1) First recall the construction of  $\log_{\mathcal{A}'}$  as in [18], §1. The generic fiber of  $\widehat{\mathcal{A}'}$  is the formal group  $\widehat{A}_L$  attached to  $A_L$ . Let  $z_1, \dots, z_d$  be a system of coordinates of  $\mathcal{A}'$  at the origin  $o$  of the special fiber of  $\mathcal{A}'$  so that  $\widehat{\mathcal{O}}_{\mathcal{A}', o} \simeq \mathcal{O}_L[[z_1, \dots, z_d]]$ . Then

$$(7) \quad H^0(A_L, \Omega_{A_L/L}^1) \subset (\oplus_{1 \leq i \leq d} \mathcal{O}_L[[z_1, \dots, z_d]] dz_i) \otimes_{\mathcal{O}_L} L$$

and consists of formal invariant differentials. Let  $\omega \in H^0(A_L, \Omega_{A_L/L}^1)$ . By [13], Theorem 1, there exists a unique analytic function

$$f_\omega : \widehat{\mathcal{A}'}(\pi_L \mathcal{O}_L) \simeq (\pi_L \mathcal{O}_L)^d \rightarrow L$$

such that  $f_\omega(0) = 0$  and  $df_\omega = \omega$  (in fact  $f_\omega$  is a formal power series, its convergence on  $\mathcal{A}'(\pi_L \mathcal{O}_L)$  is seen using the inclusion (7) above). Moreover  $f_\omega$  is a group homomorphism. The map  $\log_{\mathcal{A}'}$  is defined by  $\log_{\mathcal{A}'}(x)$  equal to  $\omega \mapsto f_\omega(x)$  for all  $x \in \widehat{\mathcal{A}'}(\pi_L \mathcal{O}_L)$ . (Note that when  $L$  is locally compact, the formal logarithm extends to  $A(L)$ , see [18], §1).

If  $\omega$  is invariant by  $G$  (e.g.  $\omega \in H^0(A, \Omega_{A/K}^1)$ ), then for any  $\sigma \in G$ ,  $d(\sigma^* f_\omega) = \sigma^*(\omega) = \omega$ . By the uniqueness property, we get  $\sigma^* f_\omega = f_\omega$  (that is,  $f_\omega(\sigma(x)) = f_\omega(x)$  for all  $x \in \widehat{\mathcal{A}'}(\pi_L \mathcal{O}_L)$ ). For all  $\sigma \in G$ , and all  $x \in \widehat{\mathcal{A}'}(\pi_L \mathcal{O}_L)$ ,  $\sigma^*(\log_{\mathcal{A}'}(x)) - \log_{\mathcal{A}'}(\sigma^*(x))$  is an  $L$ -linear form which vanishes at  $H^0(A, \Omega_{A/K}^1)$ , so it is equal to 0 and  $\log_{\mathcal{A}'}$  is  $G$ -equivariant.

(2) We have to show that the image of  $\log_{\mathcal{A}'}$  is a sub- $\mathcal{O}_L$ -module. Using a basis of  $H^0(A_L, \Omega_{A_L/L}^1)$  over  $L$ , we can identify  $\log_{\mathcal{A}'}$  to a formal logarithm  $\widehat{\mathcal{A}'}(\pi_L \mathcal{O}_L) \rightarrow L$  as in [24], IV.5. And our statement comes from [24], Theorem IV.6.4(b) in the case of elliptic curves. For the general case, see [27], §2.4, p. 196<sup>3</sup>.  $\square$

<sup>3</sup>We thank Jilong Tong for this reference.

**Proposition 8.4.** *Suppose  $K$  is complete with  $\text{char}(K) = 0$  and residue characteristic  $p \geq 0$ . Let  $h = 2[v_K(\mathfrak{D}_{L/K})]$  and let*

$$m + 1 > h + v_K(p) - 1 + \frac{v_K(p)}{p - 1}.$$

( $m \geq 0$  if  $p = 0$ .) *Let  $A$  be an elliptic curve over  $K$  and let  $\mathcal{A}'$  be its Néron model over  $\mathcal{O}_L$ . Then for any  $G$ -equivariant section  $t_m \in \mathcal{A}'(\mathcal{O}_L/\pi^{m+1}\mathcal{O}_L)^G$  of  $\mathcal{A}'$ , there exists a  $G$ -equivariant section in  $\mathcal{A}'(\mathcal{O}_L)^G = A(K)$  whose image in  $\mathcal{A}'(\mathcal{O}_L/\pi^{m+1-h}\mathcal{O}_L)$  coincides with that of  $t_m$ .*

*Proof.* Let  $\widehat{\mathcal{A}'}$  be the formal group over  $\mathcal{O}_L$  attached to  $\mathcal{A}'$ . Let  $r$  be the smallest integer  $\geq h/v_K(p)$ . For all integers  $n > rv_K(p) \geq 0$ , we have a canonical commutative diagram with exact horizontal lines

$$\begin{array}{ccccccc} 0 & \longrightarrow & \widehat{\mathcal{A}'}(\pi^n \mathcal{O}_L) & \longrightarrow & \mathcal{A}'(\mathcal{O}_L) & \longrightarrow & \mathcal{A}'(\mathcal{O}_L/\pi^n \mathcal{O}_L) \longrightarrow 0 \\ & & \downarrow & & \text{id} \downarrow & & \downarrow \\ 0 & \longrightarrow & \widehat{\mathcal{A}'}(\pi^n p^{-r} \mathcal{O}_L) & \longrightarrow & \mathcal{A}'(\mathcal{O}_L) & \longrightarrow & \mathcal{A}'(\mathcal{O}_L/\pi^n p^{-r} \mathcal{O}_L) \longrightarrow 0. \end{array}$$

Taking Galois cohomology, we get

$$\begin{array}{ccccc} \mathcal{A}'(\mathcal{O}_L)^G & \longrightarrow & \mathcal{A}'(\mathcal{O}_L/\pi^n \mathcal{O}_L)^G & \longrightarrow & H^1(G, \widehat{\mathcal{A}'}(\pi^n \mathcal{O}_L)) \\ \text{id} \downarrow & & \downarrow & & \downarrow f_{n,r} \\ \mathcal{A}'(\mathcal{O}_L)^G & \longrightarrow & \mathcal{A}'(\mathcal{O}_L/\pi^n p^{-r} \mathcal{O}_L)^G & \longrightarrow & H^1(G, \widehat{\mathcal{A}'}(\pi^n p^{-r} \mathcal{O}_L)). \end{array}$$

So it is enough to show that  $f_{n,r} = 0$  when  $n > rv_K(p) + v_K(p)/(p - 1)$ . By Lemma 8.3(2), we have a commutative digram

$$\begin{array}{ccccc} \widehat{\mathcal{A}'}(\pi^n \mathcal{O}_L) & \longrightarrow & \pi^n \mathcal{O}_L & \xleftarrow{\cdot \pi^n} & \mathcal{O}_L \\ \downarrow & & \downarrow & & \downarrow \cdot p^r \\ \widehat{\mathcal{A}'}_L(\pi^n p^{-r} \mathcal{O}_L) & \longrightarrow & \pi^n p^{-r} \mathcal{O}_L & \xleftarrow{\cdot \pi^n p^{-r}} & \mathcal{O}_L \end{array}$$

where the horizontal arrows are isomorphisms. So the canonical map  $f_{n,r}$  can be identified with the multiplication-by- $p^r$  map on  $H^1(G, \mathcal{O}_L)$ . This is the zero map by Proposition 3.7(2), thus  $f_{n,r} = 0$ . As  $rv_K(p) \leq h + v_K(p) - 1$ , the proposition is proved.  $\square$

## REFERENCES

- [1] M. ARTIN, *On isolated rational singularities of surfaces*, Amer. J. Math. **88** (1966), 129-136.
- [2] B. BENNETT, *On the characteristic functions of a local ring*, Ann. of Math. **91** (1970) 25-87.
- [3] S. BOSCH, W. LÜTKEBOHMERT AND M. RAYNAUD, *Néron models*, Ergebnisse der Math. **3**. Folge, Bd. 21, Springer, 1990.



- [4] A. BRUMER AND K. KRAMER, *The conductor of an abelian variety*, Compositio Math. **92** (1994), 227-248.
- [5] C-L. CHAI, *Néron models for semiabelian varieties: congruence and change of base field*, Asian Journal of Math. **4** (2000), 715-736.
- [6] C-L. CHAI AND J-K. YU, *Congruences of Néron models for tori and the Artin conductor*, With an appendix by E. de Shalit, Ann. Math. **154** (2001), 347-382.
- [7] P. DELIGNE, *Courbes elliptiques: Formulaire (d'après J. Tate)*, in Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 53-73, Lecture Notes in Math., **476**, Springer, Berlin, 1975.
- [8] M. DESCHAMPS, *Réduction semi-stable*, in Séminaire sur le pinceaux de courbes de genre au moins deux, ed. L.Szpiro, Astérisque **86** (1981), 1-34.
- [9] B. DE SMIT, *The different and differentials for local fields with imperfect residue fields*, Proc. Edinburgh Math. Soc. **40** (1997), 353-365.
- [10] B. EDIXHOVEN, *Néron models and tame ramification*, Composito Math. **81** (1992), 291-306.
- [11] R. ELKIK, *Solutions d'équations à coefficients dans un anneau hensélien*, Ann. Sci. ENS **6** (1973), 553-603.
- [12] W. FULTON, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Ann. Math. **90** (1969), 542-575.
- [13] T. HONDA, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), 213-246.
- [14] J. LIPMAN, *Rational singularities, with application to algebraic surfaces and unique factorization*, Publ. Math. IHES **36** (1969), 195-279.
- [15] Q. LIU, *Algebraic Geometry and Arithmetic Curves*, Oxford graduate texts in math. **6**, Oxford University Press, paperback new edition 2006.
- [16] Q. LIU, D. LORENZINI AND M. RAYNAUD, *Néron models, Lie algebras, and reduction of curves of genus one*, Invent. Math. **157** (2004), 455-518.
- [17] D. LORENZINI, *Models of curves and wild ramification*, Pure Appl. Math. Q. **6** (2010), no. 1, *Special Issue: In honor of John Tate, Part 2*, 41-82.
- [18] D. LORENZINI AND T. TUCKER, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), 46-77.
- [19] H. LU, *Isomorphism classes of special fibers of minimal regular models of elliptic curve*, preprint (2011).
- [20] T. SAITO, *Conductor, discriminant, and the Noether formula of arithmetic surfaces*, Duke Math. J. **57** (1988), 151-173.
- [21] S. SEN, *On automorphisms of local fields*, Ann. Math. **90** (1969), 33-46.
- [22] S. SEN, *Integral representations associated with  $p$ -adic field extensions*, Invent. Math. **94** (1988), 1-12.
- [23] J-P. SERRE, *Local Fields*, Grad. Texts in Math. **42**, Springer-Verlag, New York (1977).
- [24] J. SILVERMAN, *The Arithmetic of Elliptic Curves*, Grad. Texts Math. **106**, Springer, New York-Heidelberg-berlin, 1986.
- [25] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts Math. **151**, Springer, New York-Heidelberg-berlin, 1994.
- [26] J. TATE, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Lect. Notes in Math. **476**, 33-52.
- [27] —,  *$p$ -divisible groups*, in Proceedings of a Conference on Local Fields (Driebergen, 1966), Springer, 158-183.
- [28] E. VIEHWEG, *Invarianten der degenerierten Fasern in lokalen Familien von kurven*, J. Reine Angew. Math **293** (1977), 284-308.

ACADEMY OF MATHEMATICS AND SYSTEMS SCIENCE, NO. 55, ZHONGGUANCUN EAST  
ROAD, BEIJING 100190, CHINA

*E-mail address:* `huajun@amss.ac.cn`